Council of the European Union

Brussels, 12 May 2016
(OR. en)

8848/16

LIMITE

JAI 378
COSI 82
FRONT 206
ASIM 72
DAPIX 73
ENFOPOL 138
SIRIS 80
DATAPROTECT 52
VISA 144
FAUXDOC 19
COPEN 149

NOTE

From:	Europol
To:	Standing Committee on Operational Cooperation on Internal Security
Subject:	Europol contribution on improving the EU information exchange architecture and interoperability in the fight against terrorism and serious and organised crime

Delegations will find attached the contribution of Europol on improving the EU information exchange architecture and interoperability in the fight against terrorism and serious and organised crime.

The Hague, 2 May 2016

EDOC - #827969

Europol contribution on improving the EU information exchange architecture and interoperability in the fight against terrorism and serious and organised crime

1. Aim

Europol welcomes the efforts of the Presidency and the European Commission to revitalise the approach towards information exchange and interoperability. By providing this contribution, Europol wishes to support the debates at the EU level. Europol invites the Presidency to take the elements outlined in this paper into account when preparing the draft roadmap on information exchange and interoperability which is scheduled to be considered by COSI on 17 May 2016. Europol is available to provide further input to the work of the Presidency and to the high level expert group to be established by the European Commission.

2. The challenge

The following law enforcement activities can be regarded as vital in the fight against terrorism and serious and organised crime:

1. **Border control;**
2. **Information and intelligence sharing;**
3. **In-depth analysis to support criminal investigations and operational actions.**

To facilitate and supplement those activities a secure **information exchange** mechanism is needed to request additional information, follow up a hit or disseminate the results of analysis.

Each of the above-mentioned activities has different characteristics: Border controls must be fast, simple, involving minimum data (hit/no-hit) and with clear instructions for further action; '2nd line verification' or support for an on-going investigation allows for more time and requires access to more detailed data; intelligence sharing requires additional security and confidentiality mechanisms; in-depth analysis (conducted only for prioritised cases) achieves the best results but requires even more time and access to complete data sets.

There is no single EU information management tool which would be able to fully accommodate all of the needs related to the above mentioned activities. Additionally, there is much fragmentation of relevant data, as it is held in many disconnected databases.

A deeper analysis is needed on the purpose limitations of systems such as VIS and EURODAC to make them more usable to law enforcement authorities and Europol. Such analysis should focus on the needs of the user community.

A consistent approach towards the use of existing systems is needed to ensure that information is available in a timely manner to those who need it: border guards, police officers, customs officers, investigators or analysts. The selected approach should provide maximum efficiency and security while ensuring minimal effort for the end users.

3. The short term solution: '3-tier approach'

Europol and several Member States has been advocating, in particular in the fight against 'Foreign Terrorist Fighters' (FTF), for the '***3-tier approach'***, which would combine the strengths of the SISII, the Europol Information System (EIS) and Europol's Analysis Work Files (AWFs). Each of the mechanisms has its own strong points and unique capabilities, and their simultaneous use could produce significant synergies and reduce the risk of missing information. The concept would allow for the future connection of other relevant systems (e.g. VIS, EURODAC, PNR, INTERPOL databases and the possible future EES and EU Travel Information and Authorisation System) as required.

While **SISII is a very effective hit/no-hit system** for border controls, it is not meant to hold and cross-match the telephone numbers, email addresses and/or credit cards used by suspected terrorists, or to share highly sensitive intelligence or information from non-Schengen cooperation partners.

The AWF/Focal Point 'Travellers', part of Europol's European Counter-terrorism Centre (ECTC), holds large amounts of relevant data and can **support in-depth analysis** such as linkage, social network or forensic analysis. An important capability is its ability to detect links/connections between serious and organised crime (e.g. facilitated illegal immigration) and terrorism through a cross-matching mechanism. However, the most important feature of AWFs and their Focal Points is the 'human element'. AWFs are first and foremost groups of highly-qualified specialists, analysts and translators who, in addition to advanced analysis can also provide operational support (incl. on the spot with Europol's 'mobile office'), coordination, expert advice or translation. On the other hand, AWFs are designed as secure, closed environments, which are directly accessible to a limited number of authorised Europol staff and to a limited extent (in an index form) to Member States' Liaison Officers based at Europol.

The **EIS** is best positioned to serve as the central repository of law enforcement data for sharing and cross-matching purposes, including **the consolidated list of all known/suspected 'Foreign Terrorist Fighters' and their supporters**. The EIS is able to store, share and cross-match not only biographical data (name, alias, date of birth, etc.) but also other 'cross-matchable' objects facilitating the detection or identification of 'FTFs' e.g. firearms, photos, telephone numbers, email addresses, IP addresses, ID documents, vehicles, credit cards, etc. The EIS also supports to a limited extent the sharing and cross matching of biometrical data: DNA and fingerprints[1].

The EIS is directly available to all Member States, **including a growing number of national CT units**. It has the functionality of automated and real-time notifications which are sent to the owners of information in case of hits. Moreover, the EIS legal framework makes it possible to hold and make available for Member States data received from non-EU countries with an operational cooperation agreement with Europol (e.g. the United States of America, Canada and Western Balkans countries). As non-EU countries do not have direct access to EIS, Europol manages the data on their behalf, strictly adhering to any restrictions (e.g. handling codes) imposed by the Member States owning the data.

[1] Fingerprints can be stored as attachment facilitating the verification of an identity of a person but not subject of AFIS-like cross-matching.

4. Further perspectives

4.1. Easy access to information by 'single search'

The 'single search' is a core element of the Commission's Communication on 'Stronger & Smarter Information Systems for Borders and Security' of 6 April 2016. User friendliness and quick access to the information held in different relevant databases is of paramount importance for any law enforcement activity.

In response to this need, in the framework of the ISF-funded UMF3 programme led by Germany, Europol is developing the **Universal Message Format (UMF)-compliant system interface QUEST** in a pilot project with EE, ES, FI, EL and PL, allowing automatic searches of the EIS via the national databases of these countries. Europol is also exploring the legal and technical possibilities of searching the index of its Analysis Work Files via the same solution. Ultimately, QUEST should allow Member States to search 'in one go' SISII, EIS, the index of AWFs and relevant national databases. Several other Member States expressed their readiness to implement QUEST as soon as it is operational. The development of QUEST is on-going, and the first tests are scheduled for the end of 2016. The initial version of QUEST would allow a search on 'PERSON' – later also FIREARM, ID DOCUMENT, MEANS OF TRANSPORTATION and MEANS OF COMMUNICATION will be searchable. As an overall target, all relevant databases should be included in the single search interface. It is crucial that any joint interface is compatible with the UMF standard.

4.2. Easy data entry by 'data loaders'

Currently, in order to insert basic data on an individual for example 'FTF' into SISII, EIS and AWF the same data has to be inserted 3 times. 'Single data entry' is still not common in Member States for various reasons (organisational obstacles, lack of interoperability, etc.). To facilitate data entry and limit the resource impact on Member States, Europol promotes the **use of semi- or fully-automated data loaders** allowing the insertion of bulk data. The '**lightweight data loader**' concept designed and supported by Europol allows for the implementation of an efficient solution with minimal effort within 2 months, and have been successfully implemented and are in use in 7 Member States. The new *Europol Regulation* with its **Integrated Data Management Concept (IDMC)** may offer new opportunities by reducing the number of data repositories and shifting the focus from 'systems processing data' to 'purposes for processing data'. Europol will invest in this effort by ensuring that its communication system (SIENA) is able to facilitate the data entry process.

4.3. Secure information exchange

One of the flagship capabilities of Europol is **SIENA – Secure Information Exchange Network Application**. SIENA connects all Member States (including communities such as Asset Recovery Offices, Police Customs Cooperation Centres and Fugitive Active Search Teams), Europol and large number of third countries and organisations. SIENA allows users to request and receive additional information in a secure manner (including the Swedish Initiative framework) or instantly warn Member States about a specific threat. In 2015 a new version of SIENA was released with a so called '*CT space'* allowing CT units direct, secure and real time communication. To date 44 CT units (all Member States and 7 third countries) have had their SIENA mailboxes created and configured. SIENA is not yet directly available to all CT units at their premises, as a significant number of CT units manage their SIENA boxes via or from the premises of their Europol National Units. Current developments concentrate on upgrading Europol infrastructure and SIENA to EU CONFIDENTIAL (scheduled to go live in second half 2016) to better meet the needs of certain communities, including CT.

4.4. Overcome fragmentation by interoperability

A lack of common standards in the past led to information management systems being built in isolation, based on differing or even non-existent standards and no vision of future interconnection. The result of this isolated development is that Member States and the EU have to pay a high price to achieve the current vision of integration and interconnection. The Universal Message Format (UMF), as a common data exchange standard, plays a very important role in this regard as an enabler of interoperability and automation. UMF should be consistently used by all Member States, relevant EU agencies and Interpol. The target situation would be that **all relevant systems in the EU speak the same 'UMF language'.**

4.5. Cross-checking information from non-EU countries through Europol

Europol is well placed to detect and inform Member States of any external threats or connections which otherwise might have not been identified through other channels. Therefore, Europol is planning to **systematically cross-check biographic data held in SISII against data received from Third Parties (non-EU countries)**. In the long term, the same service could apply to biometric data exchanged in the framework of Prüm, VIS, EURODAC – Europol could be 'plugged-in' to Prüm as the 29th partner. An example of the requirement for this type of cross check is the fact that recently a third party offered to provide Europol with fingerprints seized from explosive devices used in past terrorist attacks. This type of data is of vital importance for the safety of EU citizens and should in the future be cross-checked through Europol's AFIS, SISII, Prüm (suspects/convicts), VIS (visa applicants) and EURODAC (asylum seekers/illegal immigrants). Unfortunately, current legal and technical limitations do not allow cross-checking most of those databases, as such cross-checking would require legislative changes and further technical improvements.

Europol, the EU information hub for law enforcement information, should fulfil this function by cross-checking several databases on behalf of Member States or on its own initiative to support Member States' investigations. It is important to note that Europol applies the strictest rules in case of hits between third party data received by Europol and data in SISII (in future VIS and EURODAC): only the Member State concerned is informed about the hit and they are always asked for permission to share the hit with the concerned third party.

Despite the current legal limitations, Europol intends to review its business processes and technical solutions regarding access to large-scale EU IT systems such as SISII, VIS, EURODAC, incl. its 'biometric matching' capabilities. As a first step, **'batch search' functionality** will be implemented in 2016, allowing systematic and semi-automatic cross-matching of relevant data received by Europol from Third Parties against SISII. In addition, Europol is **increasing its capabilities in biometrics** by hiring additional staff.