Council of the European Union

Brussels, 14 October 2016
(OR. en)

13258/16

LIMITE

JAI 831
CATS 77
DAPIX 168
ASIM 134
JURINFO 46

NOTE

From:	Presidency
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	15701/1/14 REV 1, 10824/16
Subject:	Renewed Information Management Strategy (IMS) - 5th action list - State of play

Upon proposal from DAPIX, the Council approved Conclusions on a renewed Information Management Strategy (IMS) on 18 December 2014[1] . This Strategy is aimed at managing and exchanging law enforcement information across borders in a coherent, professional, efficient and cost-effective way. The Conclusions set out that steps should be taken to develop and update as necessary a detailed IMS action list in order to fulfil the overall aims and objectives of the Strategy.

The 5th IMS action list with a 18 months life span starting on 1 July 2016 contains nine actions. These actions are referred to in the Internal Security Strategy (ISS) Implementation[2] paper as well as in the Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area.[3]

[1] 15701/1/14 REV 1
[2] 11001/1/16 REV 1
[3] 9368/1/16 REV 1

At its meeting on 28 September 2016, COSI endorsed the ISS Implementation paper. DAPIX activities mentioned in this context are the Prüm monitoring and specific IMS activities (see 11001/1/16, pg. 26).

The Council agreed that COSI will monitor the implementation of the Roadmap. Progress on the implementation of the Roadmap will be reported to the Council (JHA) of 18 November 2016 by COSI. The Roadmap refers in its chapter 2 to actions dealt with by DAPIX in the IMS framework.

In order to facilitate the above reporting, the Presidency invites delegations to endorse the current document, which takes stock of ongoing projects and progress made on the action points of the 5th IMS action list.

Action 1: A.T.H.E.N.A. SPOC training[4]

The policy of effecting as much information exchange as possible through a SPOC has been implemented by nearly all Member States although the understanding of what defines a SPOC seems to vary among the Member States. At several occasions, Member States raised the issue of specific training of SPOC staff. This action aims at identifying **training needs** and at establishing a dedicated **SPOC-network** to tackle pragmatically common operational problems in SPOCs by:

- Comprehensive training on the different EU police communication channels and EU information exchange mechanisms and instruments;

- establishing, together with Cepol, of a repository of good practices regarding training on EU law enforcement information exchange, taking into account related existing curricula and results of related initiatives (such as the Infopolex Coordination Initiative);

- exchanging best practices regarding the functioning of SPOCs, and/ or establishing a format for regular contacts of heads of SPOC/ SPOC staff, focusing on training needs and activities; and

- identifying common workflow requirements for SPOCs in the Member States and developing related guidelines as a basis for SPOC staff training.

A kick off meeting for the project is scheduled for November / December 2016.

[4] 6770/16

Action 2: ADEP (Automation of Data Exchange Processes)[5]

The main activity of daily police information exchange between National Contact Points (NCP) consists primarily of checking whether relevant data are available in the general databases of the requested Member State(s). The ADEP (Automation of data exchange process) project aims at improving and/or automating this first checking process. The project aims at smoothening data exchange through automation and restructuring of manual activities, based on an automatically generated reply protocol (hit/no hit). It is recommended to automate the current requests for information by:

- consulting an « index » provided by each Member State;
- using a standard transliteration interface, such as the one used in the SIS or in the EIS;
- giving preference to the UMF technology used by SIENA;
- taking into account the information exchange with Europol; and
- allowing MS to set up their connection to the system at their own pace.

Post-hit information exchange should be done on the basis of Council Framework Decision 2006/960/JHA ("Swedish Framework Decision").

Member States participating in the pilot project and Europol will soon organise test runs with real data. Subsequently, the impact on operational, legal and technical issues will be analysed.

[5] 14944/12

Action 3: PNR DEP (Passenger Name Record Data Exchange Pilot)[6]

The ultimate goal of this project is to provide possible solutions for the technical implementation of PNR data exchange between PIUs (Passenger Information Units). The project is based on the leading principles for interoperability and data exchange between national PIUs agreed at the UK Conference on Passenger Data on 3 October 2014.

With a view to carrying out a **comparative study** on legislation and practices governing the functioning of national PNR systems, a questionnaire was sent to Member States in April-May 2016. The **first expert meeting** (16-17 June 2016 in Vilnius, Lithuania) discussed the preliminary findings of this survey and the participants agreed that a common interpretation of the EU PNR directive and its harmonised implementation into national legislations was fundamental for an effective PNR data exchange . Participants also shared views on the data, information to be exchanged (e.g. PNR data, historical data, results of risk analyses, (common) risk profiles), on the most convenient business process and technical solution of data exchange (hit/no-hit solution, bilateral inquiries, Match3 technology, SIENA, etc.) and on the possible role of Europol.

The draft study incorporating the findings of the meeting is carried out by the Lithuanian project partner and is planned to be circulated prior to the **second expert meeting** in Sofia on 17-19 October 2016. The meeting will focus on:

- legal provisions of the PNR Directive and processes applied for the data exchange and cooperation;
- common interoperability solution, correlation and differences in the national solutions (collecting, transferring, processing, data storage, analysis, organization);
- data exchange platforms; and
- standard infrastructure requirements and agreement on the pilot infrastructure.

The study should be finalised by November 2016.

[6] 6857/16

Action 4: Enhance Information quality[7]

The 5th action list prepared on foot of the Information Management Strategy for EU Internal Security was submitted to DAPIX in June 2016 and became applicable on 1 July 2016. Objective 4 on the list is the enhancement of information quality in IT systems. eu-LISA has been invited to lead work undertaken in this regard. An action plan is proposed to DAPIX for their further assessment planning work to the end of 2018.

The importance of data quality in large-scale IT is known and acknowledged, with poorer quality data leading to higher error rates, increased manual work and resulting operational inefficiencies and, in the worst instances, inappropriate actions on the part of end-users fed misinformation. Yet analyses have demonstrated that the quality of data in eu-LISA systems could, at least in some instances, be improved. Issues encountered include inappropriate use of data fields, data inconsistencies, use of incorrect data formats, insertion of records with missing data and insertion of poor quality biometric samples. A plan is proposed with four separate work streams:

1. Enhanced detection of data quality issues at end user level

This will encompass improved detection of data quality issues to the end user allowing flagging of possible quality issues with alphanumeric data during the input process or at least better feedback on issues that can be easily remedied as well as better control of biometric data quality through the provision of standard user kits. It is felt that both actions can provide for deliverables in the short term – hence, the introduction of improved detection of issues in SIS II is considered as a possible quick-win scheduled for Q1/Q2 2017 while deployment of a user kit for biometric quality checks on data being submitted to Eurodac could also be examined in 2017. Additionally, the project will consider examination of how implementation of checks at interface level, deployment of standardised architectures with in-built quality checks or even introduction of standard devices within these setups might contribute to data quality improvements.

[7] 13301/16

2. Increasing data quality control at central levels

Improved checks at the central IT level may involve reviewing the existing Interface Controls (ICDs) as well as the deployment of data quality firewall solutions within in-stream data check/correction capabilities. Harmonisation of checks across all IT system would bring further benefits in terms of harmonised measurement of issues and implementation of remedies and could be achieved through implementation of a data warehouse reporting solution.

The need for work under work stream 2 will be assessed in early 2018, at which point the quick wins within work stream 1 should be implemented and their value clear.

3. Training of end users to better ensure data quality

Work will involve the update of continuous professional development curricula as necessary to ensure appropriate attention is given to data quality issues so that end users are equipped to provide optimal biographic and biometric data to systems.

4. Analysis and improvement of processes necessary to better ensure data quality

Processes in which data input into the systems will be compared and analysed in order to ensure an exchange of lessons learned and the elaboration of best practices that can guide any appropriate process adaptation. Where changes to processes are recommended, the resultant changes in the quality of data input will be monitored using the tools developed in work streams 1 and 2 in order to provide quantitative feedback. A comprehensive improvement in the quality of data in large-scale IT in Europe generally will require efforts from the various operators and end users involved. The involvement of Europol, Eurojust, Frontex and Member States will be required in this regard. The contribution of the Commission (DG HOME) is also needed, especially in the light of the High Level Expert Group on Information Systems and Interoperability, which is also discussing similar topics.

DAPIX is invited to consider the action plan. In case of a positive opinion being provided, eu-LISA will set out a more comprehensive and detailed project roadmap with further information regarding total budget estimates.

Action 5: UMF 3 (Universal Message Format 3) [8]

The UMF (Universal Message Format) is a European standard to facilitate effective information sharing and information exchange in the law enforcement area. It defines how communication between police information systems of the Member States as well as international systems like the Europol Information System (EIS) is to be shaped.

The current project UMF3, which is led by Germany, comprises three main objectives:

- **Stream 1: Further development of the contents of the UMF standard**

For the pilot implementation (see stream 3) the project partners were first focusing on the query and exchange of personal data, such as names and date of birth only. Now also the exchange of data related to objects (e.g. firearms, documents) is of high relevance. Therefore, the UMF3 team is currently in contact with the project members and national experts working, inter alia. on a UMF compliant firearm model. Additional requirements will be covered by further versions of the UMF standard.

Important milestones: collection and analysis of UMF requirements completed by summer 2016; next milestone: Dec 2016, new UMF candidate.

- **Stream 2: Establishing a European governance model to sustainably maintain the standard**

UMF3 team is aimedat establishing stable governance structures, even beyond the current project time span. This does not only comprise the safeguarding of long-term operational and the technical development of UMF, but also a mechanism which makes the standard and its application mandatory when developing new or adapting existing systems in the future.

Important milestones: collection and analysis of governance requirements to be finalized by autumn 2016; development of governance structures until Q3/2017; agreement on a governance structure in Q1/2018.

[8] 6882/16

- **Stream 3: Pilot implementation (Europol, Estonia, Finland, Greece, Poland and Spain)**

The participating Member States will be able to simultaneously query their national systems and EIS using the UMF standard. This will also contribute to their preparation once other EU-wide IT systems are ready to use UMF. Europol, therefore, develops a UMF-compatible interface named QUEST, which also supports the wider concept of a "Single Search Interface (SSI)" as introduced by the European Commission.

Important milestones: successive analysis, design, development, testing and go live until Q4/2017.

Standardization, put into practice under daily work conditions by the UMF3 project, is one of the main conditions to substantially improve the interoperability of EU information systems, both on technical and operational level. All three work streams are on schedule and on budget. The UMF3 project is intended to be finalized by March 2018.

Action 6: Prüm DNA post-hit procedures[9]

The purpose of IMS action 6 is to analyse the procedures applied by the Member States' law enforcement authorities following a hit in other Member States' DNA registers. The subsequent post-hit procedures (second step) include firstly, the validation and the identification of evidential value of the profile (commonly known as validation phase), and secondly, the supply of further personal data and other information upon request (commonly known as follow-up).

Until 2012, IMS action 6 has focused on the validation phase of the so-called post-hit procedures. Answers concerning national practices were received only from a limited number of Member States operational at the time when the survey was carried out. However, complementary reports which give an overview of the national procedures applied are available from other projects. In the light of these reports, it appears that the validation phase is sufficiently examined.

9 5113/12

In the context of IMS action 6 since the spring of 2016, further work has been carried out to get a more comprehensive picture of the variety of procedures for the supply of further personal data and other information in an effort to see whether national legislation could be a factor slowing down law enforcement information exchange. In order to identify commonly encountered business obstacles, a targeted research was carried out based on a questionnaire on the daily follow-up data exchange in April and May 2016. The purpose was to examine whether expedite information exchange is hampered by either current national legislation or by not applying best practices, or by other factors such as technical challenges.

A response was received from 12 Member States, which provides a sufficient basis to proceed with an analysis. On the basis of the summary of responses, an analysis is made before the end of October 2016 to draw conclusions and to propose good practices for the post-hit procedures for the supply of further information. The final report concluding IMS 6 is scheduled to be prepared by December 2016.

Action 7: PCCC: European dimension[10]

The role played by the Police and Custom Cooperation Centres (PCCC) in cross-border cooperation is constantly increasing and has been backed up by the "Paris Declaration" of 29 August 2015.[11] Furthermore, the renewed EU Internal Security Strategy (ISS)[12] reiterated the need for stepping up information sharing and operational cooperation, and the ensuing ISS implementation paper [13] underlined the goal to further strengthen the European dimension of PCCCs by exchanging their expertise. Action 7 is supported by the German Federal Police led ISF project "Strengthening PCCC Activities in the European Union".

[10] 5131/16
[11] 11594/15
[12] 9798/15
[13] 10854/1/16 REV 1

Further to PCCC staff exchange activities and training topics (identification of false documents, use of the Europol platform for experts, blended English language and PCCC training courses on the CEPOL platform), the main topics on the agenda of the 7th Annual PCCC Conference in The Hague on 11 - 12 October 2016 referred to progress made on the following specific IMS action points:

- **Implementation of SIENA in interested PCCCs**:

The implementation of SIENA in PCCCs has been brought forward. Since the start at the EPICC Heerlen (meanwhile located at Kerkrade, Netherlands), five additional PCCCs have implemented SIENA for their so called “point to point” communication between their national delegations. Latest figures by Europol show that more than 30% of SIENA cases and up to 10% of SIENA messages are meanwhile generated by PCCCs, showing the huge potential of SIENA for PCCCs in Europe.

To harmonise the use of SIENA by PCCCs as well as to define the common interests in this regard, an “Informal Group of PCCCs using SIENA” was set up. Two meetings in 2016 were held at Europol, in which Member States and Schengen Associated States intending to start in the near future the implementation of SIENA in their PCCCs participated. A roll-out of SIENA to PCCCs with French, Italian, Luxembourg, Polish, Spain and Switzerland participation is already announced for the year to come. In addition, an OSCE led project is focusing on the use of SIENA by PCCCs at the Western Balkan area.

Two meetings of the “Informal Group of PCCCs using SIENA” defined PCCC requirements as to the further development of SIENA. Especially the multilevel security approach by Europol, offering as well the so called Basic Protection Level for information exchange via SIENA, would offer possibilities to introduce SIENA by Member States whose PCCC delegations fall under very restrictive national legislation regarding the use of SIENA. The results of the meetings will be the basis for a workshop in the first quarter of 2017 to define best practices for information exchange by and via PCCCs

- **Specific analysis of cross-border crime :**

The outcome of a survey by the Austrian and Belgian delegation on cross-border crime analysis by PCCCs will be comprehensively discussed in the beginning of 2017 at workshop including PCCCs, Europol and national central services. The aim will be to increase the number of PCCCs carrying out analysis as well as to step up the level of analysis done by PCCCs from step one (exchange of statistics related to border regions) to step two (analysing exchanged statistics already at PCCCs) to step three (possessing thorough analysis up to initiating criminal investigations).

Action 8: Strengthen SPOCs

Action plan still to be defined.

Action 9: Europol's involvement in Prüm information exchange

Action plan still to be defined.