Council of the European Union

Brussels, 28 September 2017
(OR. en)

10879/17

LIMITE

DAPIX 266
ENFOPOL 341
CRIMORG 140
ENFOCUSTOM 178
AVIATION 99

NOTE

From:	Hungarian delegation
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	6857/16
Subject:	Information Management Strategy - Action 3 - Passenger Name Record Data Exchange Pilot (PNRDEP) - Final report

1. Introduction

The Council Conclusions on a renewed Information Management Strategy (IMS) for EU internal security (15701/1/14 JAI 897 DAPIX 175 CRIMORG 109 ENFOPOL 372) set out that steps should be taken to develop and, where necessary, update a detailed action list in order to fulfil the overall aims and objectives of the strategy.

In 2016, the Passenger Name Record Data Exchange Project (PNRDEP) has been included in the IMS actions list.

The current note is intended to summarize the main activities, findings of the PNRDEP project and to outline further steps towards the operative implementation of PNR data exchange.

2. Scope, actors

In January 2015 the Hungarian Ministry of Interior together with the State Agency for National Security of Bulgaria, the Mykolo Romerio Universitetys of Lithuania, the Polícia Judiciára of Portugal, the General Inspectorate of Border Police of Romania, the Secretariat of State for Security of Spain and Europol, as associate partner, submitted a project proposal in response to the European Commission's ISF call for proposals. Following the positive evaluation of the proposal in July 2015, the grant agreement was signed in October 2015, and the project officially was running from 1 January 2016 until 30 June 2017.

The purpose of the project was to explore the feasibility of using existing law enforcement data exchange channels for Passenger Name Record (PNR) data exchange between national Passenger Information Units (PIUs) and to offer possible solution for PNR data exchange.

Project activities were implemented by the six project partner Member States with a strong support received from Europol as an associated partner. Eu-LISA closely followed all project activities and shared its expertise with regard to the possible use of a ''SIRENE-like'' solution.

All Member States, EU agencies as well as representatives from US and Australia were invited to a number of expert meetings which gave opportunity to continuously inform all relevant actors about the advancement of the project, to openly discuss its preliminary findings and current legislative developments as well as to align understanding on PNR data exchange.

Member States provided highly appreciated remarks and comments on the draft feasibility study also in written form which was a key document and significant part of the project.

3. Implemented activities

The backbone of the project was the feasibility study drafted by the Mykolo Romerio Universitetys of Lithuania and the experiences gained through the three testing sessions (December 2016, February 2017 and April 2017), which were organised by the General Inspectorate of Border Police of Romania. Over the project implementation period, two expert meetings were held, to which all Member States, the Commission, EU agencies and third countries with experience in processing and analysing PNR data were invited.

Kick off conference

The opening conference organised by Spain took place in Madrid in February 2016. It gave the opportunity to introduce to the wider PNR community the objectives and planned activities of the project, to take stock of current similar data exchange projects (UMF-3, ADEP) as well as of existing law enforcement data exchange channels (SIENA, SIRENE, Fiu.net).

Feasibility study

The study-drafting took place between February and October 2016. Originally, one of the purposes of the study was to provide a legal analysis of national legislations, and to evaluate on that basis the level of readiness of the Member States to exchange PNR data. Therefore, the preparation for the drafting phase started with the circulation of a questionnaire among Member States participating in the ISEC funded PNR project (HOME/2012/ISEC/AG/PNR). In the meantime, the EU PNR Directive[1] was adopted. Considering the change that the Directive was bringing into the PNR related legal landscape and the future data exchange, it was decided to take the Directive as a basis for further discussions, and to take it as the starting point for the assessment of all possible communication channels in the feasibility study.

First expert meeting

The first meeting in June 2016 served to present the preliminary findings of the questionnaire circulated early 2016 among Member States as well as to exchange views on the data exchange procedure, possible actions in case of PNR data exchange and on the needs and possibilities of developing risk profiles and exchanging analytical information. Demonstrations on SIENA and Match3 capabilities were also held.

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Second expert meeting

The second expert meeting, coordinated by Bulgaria, was held in Sofia in October 2016. It provided fora for discussing the first version of the study, in which a greater focus was already placed on the analysis of the EU PNR Directive's provisions concerning the different scenarios of PNR data exchange. The study incorporated the analysis of the responses given to questionnaires aiming at identifying differences and similarities among MS PNR systems and the compatibility of these systems with the EU PNR Directive. The related discussion inevitably contributed to forming a more common understanding of the provisions of the Directive. In addition, the second part of the study contained an overview of possible international PNR data exchange solutions.

Testing sessions

The three testing sessions, organised and coordinated by the General Inspectorate of the Romanian Border Police, served to set up a work plan for PNR data exchange between project partners' PIUs, to draft the structured and formalized forms suggested for PNR data exchange using the SIRENE test channel, and finally, to exchange PNR data between RO PIU - HU PIU - BG PIU as well as between Europol and RO PIU by using SIENA. Demonstration of exchanging data with the help of the developed forms via SIRENE bureaux was also carried out. The last testing session set another precedent too, namely that a PIU carried out the crosscheck of PNR data received from Europol.

Closing conference

The closing conference, organised by the Polícia Judiciára of Portugal, in Lisbon on 7 to 8 June 2017 gave the opportunity to present the experiences gained during the testing sessions to all participating Member States, the Commission, EU agencies and third country partners. Also, it aimed at discussing the way ahead to reaching a well-functioning PNR data exchange model involving all Member States and Europol.

4. Data exchange simulation

4.1 WHAT and for WHAT purpose to exchange?

The Directive stipulates that the Member States shall ensure that the PIU transmits all relevant and necessary PNR data or the result of processing those data to the corresponding PIUs of the other Member States (Article 9.1 of the Directive). It is important to highlight the importance of the limitation of the Directive to exchange and process PNR data as collected from air carriers. Insofar, the provision only partially reflects the current position of the Members States that were inquired, with regard to their plans of sharing with other Member States, the PNR data, risk assessment results (analytical information obtained from PNR data) and data obtained from other modes of transport.

During the project, the study and subsequent discussions among participants showed that, on the one hand, some Member States would prefer to refrain themselves to share only the PNR data indicated in Annex 1 to the Directive, and, on the other hand, some would like to share additional information, e.g. analytical information obtained from PNR data, risk assessment, common profiles, supra-national targeting rules etc., since this could bring added value to the work carried out within a PIU and would be a step forward to closing the intelligence gaps between PIUs.

Therefore it was tried to separate the issues concerning to the exchange and collaboration (between PIUs).

PNR data exchange: is based on the Directive Article 9.1 and 9.2. The subject of the exchange: all data indicated in Annex I of the Directive.

Collaboration: sharing additional information, e.g. analytical information obtained from PNR data, risk assessment, common profiles, supra-national targeting rules etc. The possibility of such cooperation is not directly addressed by the Directive, but sharing all these activities could bring added value to the work conducted within the PIU as it's a step towards closing intelligence gaps between the EU PIUs.

Some Member States took the position that the exchange should only concern data that is already in the database and may not apply to the future flight information, meaning no watch list is allowed. This statement is directly linked to Article 9.2 of the Directive, which provides that exchangeable data are “data that are kept in the latter’s database”.

Furthermore, it was discussed, whether Council Framework Decision 2006/960/JHA could be the legal basis for risk profile sharing.

It was agreed during the project, that the PNR data, which is going to be exchanged during the PNR data exchange process, is not classified data by default.

4.2 Exchange scenarios

1) MS PIU to MS PIU

It is expected to be the most typical scenario**.**

The EU PNR Directive stipulates (Article 9.1 of the Directive) that all relevant and necessary PNR data on identified persons or the result of processing those data might be transmitted by the PIU to the corresponding PIUs of the other Member States.

Additionally, the PIU of another Member State has the right to request that the PIU of another Member State provide it with PNR data that are kept in the latter’s database and have not yet been depersonalized through masking and also, if necessary, the result of any processing of those data (Article 9.2 of the Directive).

Apart from the scope of data to be exchanged, the following legal issues arose in this scenario of data exchange: the refusal to provide information and no-response situation (what criteria should be used, which legislation is to be applied in the case of refusal to provide PNR data to the requesting PIU unit?). It may be foreseen that in most cases the refusal will be based on the different national legislation as the Directive remains silent on this issue. These are important questions to be addressed, since absence of procedures and agreements could lead to damage of mutual trust in cross-border data exchange. If such principles and procedures are difficult to establish while PNR data exchange is merely starting-up, the guidelines could be provided on the procedure to be used, i.e. proposing best practice(s).

2) EUROPOL to MS PIU

Europol has the right to request, on a case by case basis when this is strictly necessary, to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious crime, so far as such an offence or crime is within Europol's competence pursuant to Decision 2009/371/JHA (Article 10.2 of the Directive). Europol is only allowed to share data with another party if the data owner (original/initiating MS/PIU) gives permission to do so.

During the project, we made it clear that the other way around (PIU-EUROPOL) is not the subject of the PNR data exchange, it is rather based on the Article 6.3 a) of the EU PNR Directive.

3) MS PIU to third country PIU

Apart from the specific regulation found in international agreements concluded between the EU and respective third countries, the transfer of PNR data by Member States to third countries will be permitted only on a case-by-case basis for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime and in full compliance with data protection requirements and other conditions set out in Article 11 of the Directive.

Surveyed Member States showed a common intention to share the PNR data and/or analytical information obtained from PNR data with the non-EU Member States. The majority of the Member States mainly see it is possible on the basis of bilateral or multilateral international agreements.

However, there is no clear position on whether the Member States would share the information obtained from non-EU Member States with the Member States, this issue requires further discussions. The same applies to the procedures to be employed for the exchange of the PNR data between Member States and non-EU Member States, which requires special focus and also further discussion.

This scenario has not been simulated during the project.

4) MS Competent Authorities to another MS PIU (Emergency case – "Fast-Track")

The EU PNR Directive gives the right to the competent authorities of a Member State to request directly the PIU of any other Member State to provide them with PNR data that are kept in the latter's database only when necessary in cases of emergency and under the conditions laid down in the same Article (Article 9.3). The Directive requires that the requests from the competent authorities shall be reasoned, however, there is no common understanding among the Member States of what is a standard of a "reasoning" required by the Article. The concept of emergency also brings divergent understanding. The Member States declared that the list of the competent authorities would be defined following the implementation of the Directive by taking into account the purpose and limitations referred to therein.

This scenario has not been simulated during the project.

4.3 How to exchange? - SIENA

The general learnings showed that a slightly modified SIENA can be used both for EUROPOL-PIU and for PIU-PIU PNR data exchange.

Main findings regarding the use of SIENA:

- is already available in all Member States (and in 33 online third parties),
- is used by more than 800 Competent Authorities,
- supports all four (4) PNR data exchange scenarios mentioned above,
- is unified and maintained in centralized manner (technical-wise),
- can be used for both Law Enforcement Authorities (LEA) and non-LEA based PIUs,
- supports the information exchange up-to EU-CONFIDENTIAL level, but can also be used up to EU-RESTRICTED only,
- provides support for system to system integration through web services,

– supports the internal communication required to prepare outgoing messages or process incoming messages,

– users are identified and managed via the Identity and Access Management application,

– data and content auditing and retention policies are in place.

Furthermore, Europol foresees in the near future the implementation of a Basic-Protection-Level (BPL) in SIENA communications, which would simplify and ease the information exchange between PIUs established on different legal bases (police, border management, national security basis or established as independent units). *It is a pre requisite for SIENA communication to deploy the SIENA endpoint into the PIU facilities (during the project period HU, RO and BG successfully deployed the endpoints).*

4.4 How to exchange? - SIRENE-like solution

It is important to highlight as an output of the simulation through the SIRENE system that in case of PNR data exchange through SIRENE, it is necessary to develop/clone a „SIRENE-like solution" (central infrastructure at eu-LISA) as the SIRENE is the platform of communication among SIRENE Bureaux and it cannot be used for PNR data exchange.

Main findings regarding the use of the SIRENE-like solution:

– already established channel, functioning and successfully operating at national level,

– secure: data is exchanged over a private and encrypted network infrastructure (SIS II),

– mandatory: use as per legal basis following SISII ''hits'',

– reliable: non-delivery notices are sent if mail delivery fails,

– simple solution, based on standard technology and cost-efficient infrastructure at central level (eu-LISA),

– highly available and supported 24x7 by eu-LISA, who also offers relevant training programs to Member States,

– technically available and ‘’fit for purpose’’ to facilitate data exchange among PIUs : it is important to note, that in case of use of SIRENE for PNR data exchange, the central message-relay would have to be cloned (‘’SIRENE like’’solution) and this clone should be used for PNR data exchange,

– easy to exchange the PNR data with the support of the “PNR-form”,

– governance, business processes and organizational management already in place, agreed and used by MS, including aspects related to data quality and interoperability, covered by the SIRENE Manual. Data quality and completeness are guaranteed by the use of standardized forms.

5. Common identified challenges

5.1 Issues for PIU efficiency:

– Interoperability of IT systems – different, not interconnected systems, are used in PIU operations in international data exchange activities. PIU use the national PNR data management system for their daily operations. International requests and follow-up replies operated through SIENA require separate end-points. At the moment, in most cases, the content is transferred manually (registered, encrypted memory key can be used in some cases). Leading to:

  – Excessive time consumption, especially full response information in a “hit” case;

  – Human error, mistyping, misuse of language specific letters.

– The national PIU internal authorisation system requires an authorized person to authorise incoming requests and responses. The authorised person will be different from the one working with the SIENA end-point, meaning significant inefficiency in work organisation.

– Efficient use of human resources – flows of national PNR data are relatively easy to plan as well as the allocated resources required. International PNR data exchange flows are less predictable, can be very fluctuating, building high peaks leading to disturbance of business as-usual operations. The testing sessions showed that the "no-hit" scenario required twenty-two minutes to be fully implemented (from request appearance to sending the response).

– International data exchange vs. national operations – setting priorities (with data should be processed first in respect of limited resources), queueing rules (prioritization rules or "first-in-first-out" principle to be established) were topics for further discussions. Those two types of operations are also different in required attention and stress level (due to unplanned urgency nature in some cases) leading to shift management and more complex work time management.

– Capabilities of SIENA infrastructure – The testing sessions showed that four minutes were required to transfer the message. This delay appeared because of the way the SIENA messaging system is implemented. The SIENA messaging system is based on a queue which is read every 2 minutes. This delay doesn't impact the business process. Future versions of SIENA will further reduce the delivery time of messages.

5.2 Issues for further consideration:

– Time of response – any SLA (Service Level Agreement – setting expected time lines between processes) is agreed among MS. Testing sessions showed that processing of data about thirty persons took more than six hours. It also applies to status tracking issues (was the request received, was it justified, is it queued or processed, etc.).

– Responsibility for the analytical part – at which point (request or response) transliteration, soundex and other analytical activities should be made. Otherwise, it will not be clear in a "no-hit" case if the record was not available or whether the search was incomplete.

– Request data structure – what is the minimum / desired structure of attributes, to start next process.

– Common interpretation of “duly reasoned” or data set for justification – agreement on minimum data required for justification, should those include case number, type of crime, purpose (investigation / intelligence), etc.?

– Justification of scope of PNR data provided in response – should it be only meta-data, or a number of records (some frequent flyers might have over two hundred (200) annual records).

– Should PNR have a separate channel?

– Procedure of “no-quick-match” (provided by SIENA) should be agreed. Should the request be processed further? The same applies for the procedure of “changed or extended request”.

– Validation of data – this step is organised in different way in different ways. Should the response indicate validation sources (SIS, VIS, etc.)?

– Data quality – discussions with carriers? This also includes interpretation of empty fields and mistakes in data.

– Interpretation of Matching – Full / Partial matching, which data matches in partial matching case, non-personal data matching?

Besides the above listed issues, some more general topics can be pointed out for further considerations, also in relation to some of the recommendations of the final report of the High Level Expert Group (HLEG) on interoperability:

– Unified solution for data provision (for carriers);

– More efficient consolidation of API and PNR data;

– Possible future role of EU LISA in international PNR data exchange;

– Implementation of a new ‘’SIRENE-like’’ solution for PNR data exchange.

6. Next steps

It is important to ensure that any further steps should build on the findings and experiences gathered in the framework of the PNRDEP project in order to avoid duplication and re-discovering challenges.

PIU to PIU/EUROPOL-PIU data exchange

1. Decision about the communication channel for PNR data exchange 'PIU-PIU'

The EU PNR community should decide on the preferred channel to be used for PNR data exchange between PIUs.

2. Developing a document „Data exchange between PIUs" (description of the data exchange mechanism customized to the chosen tool (channel))

Following the decision, a "Data exchange between PIUs"-manual should be developed, which describes the data exchange mechanism customized to the chosen channel. This could include

- the PNR data exchange template (Data model),
- the UMF based data model,
- the development of a full set of business and functional requirements for international PNR data exchange, as well as technical descriptions.

Pre-requisites for developing a manual:

- Investigating the use of Swedish Initiative requests (EUROPOL, PIUs);
- The use and process implication of different handling codes;
- Expectations on response time in comparison with resource availability within the MS (and Europol);

– Possibilities for enhanced interoperability between national case management systems and the information exchange tool(s);

– The prioritisation or cross-matching of selected data sets as to ensure only the most relevant hits are shared due to resource and time implications for PIUs;

– Procedures on the exchange of other data elements contained within the PNR data;

– Formats and/or minimum requirements for included data elements to be shared.

For EUROPOL-PIU data exchange

As to the implementation of EUROPOL-PIU data exchange, the following should be considered:

– every PIU shall be able to implement SIENA by May 2018;

– achieve full establishment of the PIU network (new PIUs accounts);

– SIENA-BPL (Basic Protection Level) as a pre-requisite for points above.

– The feasibility of creating a new “isolated” information exchange system dedicated to PIUs.