COUNCIL OF THE EUROPEAN UNION

Brussels, 21 October (23.10)

14592/08

LIMITE

CRIMORG 168
AVIATION 241
DATAPROTECT 73

NOTE

from :	Presidency
to :	Multidisciplinary Group on Organised Crime
Subject :	Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes General discussion of matters relating to the analysis and transmission of PNR data and data-protection

This note sets out for delegations the questions to be discussed at the meeting of the Multidisciplinary Group on Organised Crime (MDG) on 28 and 29 October 2008, in accordance with the working method introduced following the guidelines issued by the JHA Council at its meeting on 24 and 25 July 2008. The examination of the document will be continued if necessary at the MDG's meeting on 3 and 4 November.

I - FURTHER DISCUSSION ON THE ANALYSIS OF PNR DATA IN THE PASSENGER INFORMATION UNIT FOR THE PURPOSES OF RISK ASSESSMENT

To draw the conclusions from previous discussions it is proposed that:

(1) the European instrument should contain a definition of the operations that may be authorised in connection with the PIU's risk analysis.

The Presidency considers that a definition will give the PIU greater legal certainty in its work, especially by avoiding needless suspicions. The following definition is offered for the delegations' assessment:
Risk analysis: "Automated processing of personal data to identify, within the PNR database for which the PIU is responsible, persons likely to pose a risk, on the basis of criteria founded on objective factors previously established by the competent public authorities of the Member States which make it reasonable to suppose that the persons identified by these factors are or could be involved in the preparation or commission of an offence covered by this instrument; no risk-assessment criterion may be based on a person's race or ethnic origin, religious beliefs, political opinions, membership of a trade union, health or sexual orientation; the risk analysis may also involve cross-analysis of PNR data with international, European or national files on persons or objects sought or under alert with a view to determining the action to be taken."

(2) it should be noted in the summary of conclusions of the proceedings that the MDG will consider at a later stage the question whether the European instrument should provide a backup for the national procedure for drawing up risk criteria.

- **Interconnection of the PNR database and the API database**

Discussions in the MDG have shown that the PNR/API interconnection is the condition *sine qua non* for the effective use of PNR data. The API data make it possible to broadly limit the risk of "false positives" by checking the accuracy of the identity features collected from the PNR data of airline passengers who are submitted to the risk analysis. Given the importance of such checks from the point of view of protection of fundamental rights, the Presidency considers that any doubt about the need for them needs to be removed.
Proposal: whatever legal basis is eventually chosen for the future instrument, the instrument will either have to determine the conditions for such checking or at least state in the preamble why it is essential that national law, in accordance with the authorisation given by Directive 2004/82/EC, should deal with this question.

- **Interconnection of the PNR database and files on persons or objects sought or under alert with a view to determining the action to be taken**

During the previous discussions, the MDG very broadly supported the Presidency's proposal that a clear distinction should be made between the role of PIU and the role of the law-enforcement authorities responsible for controls and investigations and that the task of carrying out the processing operations of the PNR database should be given exclusively to the PIU, for the purposes of both the risk analysis and the investigations carried out by the competent authorities.

(1) Some delegations feel there is a need to clarify the conditions for the interconnection of the PNR database and SIS-type files. There is concern that all passengers whose PNR data are covered by the instrument will be the subject of searches in those files, which might be considered to be contrary to the principle of proportionality.

The Presidency therefore suggests to the delegations that the risk analysis process be discussed in more detail, following a four-step approach:

Step 1: Selecting the flights whose PNR data will undergo an assessment of the risk posed by the passengers, in accordance with the risk analysis described below. (The selection criteria are adopted by the competent authorities.)

Step 2: PNR/API interconnection.

Step 3: Assessment of risk on the flight in question:

- **"Profiling" of PNR data**

The result generally appears as a percentage. The threshold beyond which a passenger must be regarded by the PIU as "positive" is set by the competent national authorities.

- **PNR/SIS-type files interconnection ("targeting")**. *There are various options here:*

(a1) All passengers on the flights selected are submitted to interconnection.

(a2) Only passengers deemed "positive" upon profiling are submitted to interconnection.

(b1) Interconnection is assigned to the PIU.

(b2) Interconnection is assigned to the competent authorities.

The Presidency considers that option (a2) has the disadvantage that much of the benefit of the risk analysis is lost, when the whole purpose of the PNR instrument is risk analysis; the disadvantage of option (b2) is that the PIU is deprived of virtually raw PNR data on a massive and systematic scale, and this raises the question as to which competent authority should be in charge of the interconnection.

Step 4: The personal data of passengers who have shown a positive result at Step 3 are sent by the PIU, with the corresponding API data, to the competent authorities, which will analyse the data on a case-by-case basis and take the appropriate action.

(2) One delegation has pointed out that under the legislation of some Member States access to SIS-type files is reserved for the "law-enforcement authorities" alone.
Where necessary, the future European instrument should provide for the PIU to have access to these files for carrying out the tasks assigned to it by the instrument itself. The Presidency suggests that the MDG should note that this question will have to be looked at in more detail.

II - FURTHER DISCUSSIONS ON THE TRANSMISSION OF BULK PNR DATA

At the previous meeting, a number of delegations, supported by the Commission, said it needed to be possible – in a few limited cases and in order to serve the purposes of the instrument – for bulk data to be processed by another PIU or by a competent authority in the Member State which collected the data.

- What purposes do the delegations consider could justify giving access to the PNR database to an authority other than the PIU which collected the data and was responsible for storing and analysing them?

- Depending on how they answer this question, do the delegations consider that this expanded access should be restricted to, for example, in exceptional emergencies or exceptionally serious circumstances?

- Is there also a need, for reasons of data security, to limit transfers of bulk PNR data, with preference being given to onsite access (in the premises of the PIU)?

III - PROTECTION OF THE PERSONAL DATA OF AIRLINE PASSENGERS

The Presidency offers the following proposals (o) to (v) for discussion. The aim is not to seek final agreement among delegations on the wording or technical points of the draft but appropriate guidelines on the types and levels of protection to be granted. Delegations are invited to submit additional proposals as they see fit.

(o) Rules applicable to the processing operations necessary for the transmission of PNR data by the airlines to the PIU

Queries have been raised, especially in the opinion of the European Data Protection Supervisor[1], who notes that the airlines should not have to comply with two different legal frameworks depending on the purposes for which they transmit the PNR data. This problem might be avoided by deciding to apply a protection system equivalent to the one provided for in Directive 95/46/EC.

(o.1) Proposal: whatever legal basis is eventually chosen for the future instrument, the instrument should either determine the conditions for such checking or, at the least, state in the preamble why it is eminently desirable that this question should be regulated by national law, in accordance with Directive 2004/82/EC.

(p) Common rules applicable to processing operations by the PIU and by the competent authorities

(p.1) Apply the guarantees provided for in Articles 4(6), 11, 11a, 11h and 11i of the current draft instrument, as per 7656 CRIMORG 49;

[1] Opinion 2008/C 110/01; see, in particular, paragraphs 41, 42, 53 and 60.

(p.2) Add to these Articles: The processing of personal data processed by the PIUs and the competent law-enforcement authorities under this instrument is subject to the national law of the requesting Member State. With regard to the processing of personal data consulted under this Decision, each Member State shall ensure an adequate data protection level in its national law which at least corresponds to that resulting from the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and, for those Member States which have ratified it, the Additional Protocol of 8 November 2001 to that Convention, and shall take into account Recommendation No R (87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector. (Alignment on Article 8(1) of Decision 2008/633/JHA.)

(q) Specific rules applicable to processing carried out by the PIU

q.1: Database access restricted to trained, authorised staff

- Only staff who have been individually designated and specially empowered and have followed the appropriate training mentioned below are authorised to process data stored in the PNR database.
- Before being authorised to process data stored in the PNR database, the staff of the PIU shall receive appropriate training about data security and data protection rules and shall be informed of any relevant criminal offences and sanctions. (Alignment on Article 8(8) of Decision 2008/633/JHA.)

q.2: Checking of requests before information is transmitted to the competent authorities

Before transmitting information resulting from the processing of PNR data, the PIU checks that the following conditions are met:

- a reasoned request,
- drawn up by a competent authority within the meaning of this instrument, and
- complying with the aims laid down by the instrument.

q.3: Traceability: rigorous logging of accesses and transmissions

- Apply Article 11b of the current draft instrument.
- Add: The PIU also records all accesses to the PNR database and all requests received from the competent authorities. The record must at least make it possible to identify the PIU staff member who accessed the data, the author of the request, and the date and description of the processing operations requested.

q.4: Data quality

- All reasonable steps must be taken to ensure the erasure or rectification of data which the PIU or the competent authorities have found to be inaccurate or incomplete having regard to the purposes for which they were collected or subsequently processed.

q.5: Prevention of "false positives"

Personal data resulting from risk analyses performed by the PIU are transmitted to the competent authorities so that they can decide on any appropriate action in the particular case; such data may not undergo any further processing unless it is done in the interests of the person concerned – for example, to make the necessary rectifications to eliminate "false positives" or, with the same end in view, to ensure that the risk-analysis criteria are updated.

q.6: Sanctions

The Member States lay down dissuasive, effective and proportionate sanctions for breaches of the instrument's rules on data protection and data security and the rules of national law adopted for its implementation.

q.7: Data security

- Apply Article 12 of the current draft instrument (which is aligned on the DPFD).
- Add: a provision to ensure that the PIU premises are sufficiently secure.

(r) Information, right of access and rectification, right to compensation and judicial remedy

- Apply Articles 11c to 11g of the current draft instrument
- Add: improving the instrument's transparency by two further measures:
  - informing the public with posters at airports;
  - drawing up a guide to the right of access along the lines of the guide for the Schengen Information System.

(s) Transfers of analytical data between the competent authorities of the Member States

On this point, the European PNR instrument will refer to the provisions of the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (currently being published).

(t) Transfers of analytical data or of bulk PNR data to the public authorities of third countries/international organisations

(t.1) The transfer of analytical data by a Member State's competent authorities is covered by Article 8 of the current draft instrument.

(t.2) Transfer of and access to bulk PNR data is also subject to additional restrictions made applicable to the Member States by the PNR instrument.

(u) Sensitive data

In order to have a more precise idea of the delegations' positions, the Presidency offers two possibilities for consideration:

(1) Simply banning access to sensitive data

PNR data in category 12 as referred to in the Annex to the instrument are processed by the PIU with a view to immediate erasure.

The Presidency would draw the delegations' attention to the possible disadvantages of such an approach: in certain circumstances, erasure may be harmful to a person's protection-worthy interests; a ban on all processing of any sensitive data leads to the total erasure of category-12 information.

(2) Allowing limited access

As a basis for discussion, here is a reminder of the United Kingdom's proposal:

"Article 3(2): Amend final sentence to "the Passenger Information Unit shall only process such data as referred to in Article 11a(2)."

New Article 11a(2): "Processing by Passenger Information Units of special categories of data contained within PNR data shall only be carried out on a case by case basis:

a) following completion of the automated risk assessment ;

b) where strictly necessary; and

c) when domestic law provides adequate safeguards."

(v) Period of storage of data in the PIU

Most delegations readily welcomed the Presidency's proposal that there should be a single compulsory storage period so that the requirements of European cooperation could be properly met, with an upper limit being placed on the storage period authorised throughout the territory of the European Union. Following up the earlier discussions on this point, the Presidency makes the following proposal:

- compulsory storage period for all Member States: the Presidency suggests three years;
- authorised additional storage period: the Presidency suggests seven years.