



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 28 November 2008

16457/08

**CRIMORG 208
AVIATION 286
DATAPROTECT 100**

OUTCOME OF PROCEEDINGS

from: Council
on: 27 November 2007
prev.doc. 15319/1/08 REV 1 CRIMORG 184 AVIATION 255 DATAPROTECT 86
Subject: Proposal for a Council Framework Decision on the use of Passenger Name
Records (PNR) for law enforcement purposes
– Report on thematic work carried out from July to November 2008

In accordance with the mandate given to the Presidency by the Council, at its meeting on 25 July 2008, the Presidency prepared the report below. On the basis of this report, the Council endorsed the following assessments and guidelines:

- 1) The working method followed has resulted in an increasingly clear vision of the practical scope and essential features of a possible European PNR system reconciling operational effectiveness with respect for citizens' fundamental rights in general and personal data protection rights in particular;**

- 2) The Council preparatory bodies are instructed to examine all the outstanding issues, whether legal or operational, in the light of the report and all the work already carried out with a view to decisions at a later date;**

- 3) The dialogue with the European Parliament and, in the Member States, with national parliaments and the economic operators concerned will continue in parallel¹;**
- 4) The preparatory bodies will report regularly to Coreper or to the Council, as the case may be, on the progress made in ongoing proceedings and consultations.**

¹ DE scrutiny reservation on the collection and the processing of data in the absence of concrete suspicions.

EUROPEAN PNR
REPORT ON THE THEMATIC WORK CARRIED OUT FROM JULY TO
NOVEMBER 2008

The proceedings of the Multidisciplinary Group (MDG) were organised in three sessions devoted to data collection, use of collected data and protection of air passengers' rights, respectively. On each of those subjects, ideas and arguments were exchanged and contrasted on the basis of discussion documents with a view to gradually refining the common perception of the essential features which a European PNR system could incorporate. Representatives of all the parties involved were given ample opportunity to take the floor (I) and their points of view were amply taken into account when identifying the provisional conclusions presented to the JHA Council (II).

(I) The consultations made it possible to collate a lot of useful information

(a) Hearings organised by the MDG

• Air transport operators

The MDG heard the main international and European air carrier associations (IATA with 280 members accounting for 95 % of world traffic and AEA bringing together 31 European carriers), as well as representatives from the two main companies managing PNR data on behalf of air carriers (AMADEUS, a travel booking agency, and SITA, a company providing airport computer services).

The operators testified to the growing interest which authorities responsible for border management and public security have been taking in PNR data around the globe. Transmission requirements vary from State to State. In the international context, operators are seeking the European Union's support to work towards the greatest possible harmonisation of the obligations imposed on them in order to limit the cost and the burden of legal responsibilities which they face to the minimum necessary.

The hearings revealed the considerable experience acquired by the operators and, above all, their intermediaries, in the travel data management field. As PNR develops throughout the world, technologies adapt and costs may fall. The service providers stated that a 100 % push method is perfectly feasible from a technical standpoint, irrespective of the airline, and that data on international travellers in transit in the EU can be transferred to all Member States concerned.

The cost for air carriers of transmitting PNR data to the public authorities can be estimated at between 10 and 20 euro cents per air ticket sold, depending on the technical systems used. The more those systems are harmonised for groups of transmissions, the more transmission costs can be reduced.

- **EU Counter-Terrorism Coordinator**

Mr Gilles de Kerchove relayed the views of counter-terrorism services which he had consulted. These views are that in Europe, as elsewhere in the world, PNR data are undeniably useful in the field of counter-terrorism, partly on account of the specific vulnerability of terrorists when crossing international borders and partly on account of the significant and intrinsic potential afforded by the PNR tool.

For obvious reasons, neither the figures collected nor the methods of action can be publicly disclosed. The Coordinator nevertheless stressed the usefulness to the Union, in both political and operational terms, of rapidly equipping itself with a PNR system in an international context where the number of countries adopting such a system is increasing rapidly;

- **PNR specialists within police and customs authorities**

In addition to the presentations already given in the first half of 2008, in particular by the Australian, Canadian and North American authorities, the MDG examined the question of the need for, the arrangements for the collection of and the scope for the use of PNR data by questioning in details various services responsible for security. The operational services of the PNR databases already in place in the United Kingdom were heard, as were those of the French customs authorities, the Danish national police and the Danish intelligence services and the Belgian criminal police, which use PNR data in the context of pro-active activities within the domestic legal framework.

All testified that PNR data is a key means of combating numerous forms of serious crime, particularly those susceptible to detection when borders are crossed (activities linked to terrorism, trafficking in drugs and all types of illicit product, counterfeiting, trafficking in human beings and animals, false passports, etc.). Numerous real-life examples were provided. Statistics adapted to the "PNR usefulness" question are not always available. However, the French customs authorities formally stated that each year between 60 % and 80 % of narcotic seizures at the international airports of Paris (roughly two tonnes annually) are directly attributable to the availability of PNR data.

All the experts heard considered that the concept of organised crime was insufficient to describe the field of offences covered, and inappropriate on account of the fact that the "organised" nature of the offence cannot be detected immediately and may only be uncovered later in the investigation. They also provided valuable information concerning the setting up of units (PIUs) specialised in the use of this specific tool, the possibility of carrying out risk analyses and the links between PIUs and the departments responsible for controls and investigations.

- **Agency for Fundamental Rights**

The opinion of the Agency for Fundamental Rights, requested by the Presidency following the discussion in the Council on 25 July 2008, was examined by the MDG. The MDG brought together all the points which at this stage in proceedings could provide a follow-up to the very useful recommendations formulated by the Agency.

Thus, explanations and evidence were gathered to establish the need for the projected measure, which should not be approached theoretically but on the basis of acquired experience, and its proportionality with respect to the purpose intended; definitions were identified to respond to the need for foreseeability of the measure (offences covered, arrangements for data use, profiling, etc.); careful consideration was given to information to passengers and safeguarding their fundamental rights, in particular through the granting of sufficient procedural guarantees; risks of discrimination, notably on ethnic or religious grounds, were eliminated by following the Agency's recommendations.

- **European Data Protection Supervisor**

Mr Peter Hustinx spoke to the MDG, repeating the substance of his opinion and making additional recommendations. He had been kept informed of proceedings, so that he would be able to present any comments or proposals he might have. The MDG tried to provide as many answers as possible, at this stage of proceedings, to the questions and concerns he expressed.

A significant effort was made as regards the clarification and coherence of the data protection rules applicable, since specific rules have to be identified in the instrument, in particular to ensure that the limits imposed on the use of PNR data are strictly complied with.

(b) European Parliament involvement

The French Presidency has kept the relevant bodies at the European Parliament informed in detail about the work programme being followed and the results achieved. It has made itself available to respond to their questions and to work in a concerted fashion. This report will also be forwarded to the Parliament.

This approach has borne fruit, showing that it must be continued. The European Parliament has not yet delivered the opinion requested on 10 December 2007; however, following an oral question put to the Commission at the plenary meeting on 20 October 2008, a draft "wind-up resolution" was drawn up by the LIBE Committee (to be updated following the vote in the LIBE Committee due on 17 November 2008).

The Presidency has also been careful to pass on to delegations the legitimate questions raised by members of the European Parliament. As underlined by the JHA Council at its meetings in July and October 2008, there must be a detailed dialogue with the European Parliament and national parliaments regarding the need to which this tool responds, the way in which the data is to be used, and the special protection the data must receive.

(II) Summary of results achieved

These results also include those emerging from the proceedings in the first half of 2008 under the Slovenian Presidency of the European Union.

(a) On the need for and usefulness of a European PNR instrument

- **The PNR tool offers a potential of its own.** Because of the special nature of PNR data (all information about a travel reservation) and the possibility of access to it well before the flight lands, such data is complementary to other existing control or investigation tools, not superfluous to them. Its use gives access to specific information about offenders' behaviour, such as the itineraries for and frequency of their journeys, the circumstances in which their plane tickets are bought (travel agency, means of payment, credit card details, group purchases, etc.) and other matters connected with the trip (hotel reservation, car hire etc). It makes it possible to detect offences because of suspicious behaviour, to find those suspected of crimes, to reveal links between a person and a known criminal, or links between a person and a particular criminal case.

The establishment of a PNR database offers both opportunities to analyse behavioural tendencies in criminal circles, on which basis the criminal risk on particular flights can be assessed, and opportunities to provide information for investigations by intelligence services, customs, police and the criminal justice system. It allows the proactive use of the information contained in it, with the aim of preventing crime and detecting crimes which have been committed or are being planned; also, thanks to the later use of data which has been stored, it may help to clear up unsolved crimes.

It was noted that representatives of the relevant services with experience in the PNR field, whatever their speciality, are entirely agreed on this. It should be noted that the work under way on the European PNR has promised a spontaneous reaction from the Council of Europe, whose Airports Group has expressed its full support for the projected European PNR, given the usefulness of PNR data of which the 110 expert members of that group are already aware¹.

¹ 10949/08 CRIMORG 93.

- **PNR data has already shown its worth in Europe.** This data has been used for many years throughout the European Union, under existing legislation. For example, much use is made of it by customs services working at airports. The experience of customs services demonstrates the obvious usefulness of PNR data, particularly in combating trafficking in human beings, drugs trafficking, and the smuggling of counterfeit goods etc. This effectiveness is recognised at European level, and is the subject of proceedings in the Customs Cooperation Working Party, with reference for example to the development of common methods for risk analysis.

Police services in the Union are also gaining experience, depending on the various arrangements under the national legislation in force. The domestic law of three Member States already provides for the establishment of a PNR database. In at least three others similar legislation is in preparation, at a more or less advanced stage. In most Member States, there is no PNR database, at least not a permanent one. However, many national legal systems already allow PNR data to be used proactively or for law enforcement purposes by requisitioning it from airlines.

Besides the fact that the creation of a database available to the public authorities would contribute to the more effective and better regulated use of PNR data at national level, it would also improve common security, particularly at the EU's external borders, by the sharing of the resources deployed in each Member State.

- **The establishment of a European PNR is an alternative to the steady development of different national solutions.** Its early establishment would facilitate adequate alignment of the technical solutions being implemented, thus making it possible to ensure the necessary compatibility between national systems and to encourage exchanges of good practice. A European instrument in this area would contribute to effective cooperation between the law enforcement authorities in the Member States and the application of common standards of personal data protection.

- **The benefits of having a European PNR exceed the security challenges.** As the airlines have stated, a coherent solution for the EU's 27 Member States would also be in the airlines' interests, as they have to cope with the variety of national solutions adopted around the world.

The definition of a European policy on this matter would also have a positive impact on the relationship between the EU and third States. The sooner this policy is developed, the more the Union will be able to influence the way in which the PNR data of European citizens is used during their international journeys. This is all the more important, since it is clear that PNR can be implemented not only in countries which have the same idea of respect for fundamental rights as the European Union.

(b) Consensus might be found on the creation of a decentralised system, to be phased in gradually, together with an assessment and revision mechanism.

- **A decentralised PNR system** The working hypothesis is based on the establishment of national databases which are able both to contribute to domestic security and to respond to needs formulated by other Member States. The approach of having a centralised PNR system at EU level has been rejected by a vast majority of delegations, and the Commission has refused it, particularly because of the technical complexity of such a tool which could have grave consequences for data security.

- **The European PNR may be set up where there is the broadest and clearest consensus amongst the Member States at this stage.**

Consensus is focusing on coverage of air travel between the EU and third States (including transit within Europe). The purposes would be the **prevention, detection, investigation, prosecution and punishment of terrorism, and of a group of other serious offences to be defined by reference to the list in the Framework Decision on the European Arrest Warrant.**

That list, which contains 32 categories of criminal offence, is an important reference which is already used in other EU instruments.

To avoid gaps in the collective operation of the future European PNR system, it is felt that **systematic transmission of PNR data for all flights within the scope of the instrument** is preferable to selective data collection limited to certain flights. The effectiveness of a system common to the EU's Member States would seem to depend on sufficient availability of all the data, in respect of all the Member States and throughout the storage period set by the instrument. However, so as not to close the door to revision of this approach, it was felt to be appropriate to provide for a gradual phasing in of the system, and a review clause stating that the option of systematic data collection could be re-discussed on the basis of experience gained after several years.

The solution outline here should have neither the purpose nor the effect of excluding complementary national choices, taking account of the possibilities and constraints stemming from European legislation. In this respect, possibilities include combating illegal immigration and protecting public health; covering intra-Community air transport; and covering means of transport other than aircraft. Many Member States seem to wish to maintain this freedom; some have already made such choices and there seems no valid reason why the establishment of a European PNR which responds to certain needs should make those Member States cease responding to other needs recognised at national level.

The options adopted should be viewed as a first stage, and be supplemented with assessment and review provisions, so that they can be adjusted as needed in the light of the experience which will gradually be acquired.

(c) Technical and financial constraints on the economic operators should be kept down to the strict minimum necessary

The presupposition is to impose no obligation on air carriers to collect data, but only an obligation to transmit the data they have actually and previously collected for the purposes of their commercial activities.

The collection and transmission arrangements must be tailored to the possibilities on the one side and the needs on the other: the list of data to be transmitted and the technical transmission protocols must reflect the state of the art by following the international standards set by the International Civil Aviation Organisation and applied by IATA. Furthermore, the transmission would take place – except in special cases – only twice: 48 hours before take-off, and on flight closure. The objective to resort only to the push method can easily be retained, together with a transitional period granted to airlines in order for them to bring their systems up to date. Lastly, a single set of data protection arrangements must apply to airlines whether the data are transmitted for commercial purposes or to the public authorities.

(d) PNR data must be processed in a manner which is effective and transparent and fully complies with the legislation in force

- **A Passenger Information Unit (PIU) would be set up in each Member State to act as the public authority hosting the PNR database and ensuring compliance with the rules in force.**

A consensus emerged on the principle that PIU staff members should belong to the public authorities of the Member States. The PIU should be designed as an "intelligent" platform comprising specialised staff whose task would be to meet the needs expressed by the departments responsible for checks and investigations and to liaise closely and responsively with them to this end. This would make it possible to make effective use of the PNR database while ensuring the traceability and lawfulness of the processing operations carried out.

Storage of the raw data in a secure database was deemed to be by far preferable to an approach allowing such data to be transmitted to external entities. Access to the PNR database would be restricted to individually designated officials, who would be specially trained to use the instrument in full compliance with all applicable rules. A system of appropriate sanctions would be established in each Member State to prevent and punish infringement of these rules.

The detailed arrangements regarding the structure and location of the PIUs can be adjusted by the Member States in accordance with their air traffic situation, crime structure, configuration of national law-enforcement authorities and available resources; for instance, it should be possible to set up a PIU common to several Member States in order to pool their resources.

- **A precise division of responsibilities between the Passenger Information Unit and the operational departments using PNR data to fulfil their duties was deemed to be the primary factor in ensuring the transparency of the European PNR system** – an indispensable step given the imperative to safeguard the right to privacy and protect personal data.

The list of tasks identified at this stage of the discussions would be based on the points below.

PIU: data collection from airlines; real-time analysis of PNR data relating to certain preselected flights in order to assess the possible risk posed by certain passengers; deferred-time data analysis in order to update risk indicators; analysis of the PNR database at the request of a competent authority conducting an investigation; transmission of the analysis results to competent authorities; exchange of information with other Member States' PIUs; logging of analyses performed, results obtained, requests received and transmissions made; and data storage.

Competent national authorities: definition of the criteria for preselecting the flights which will be subject to risk analysis; requests to the PIU for deferred-time data analysis in order to update risk criteria; specific requests to the PIU with a view to PNR data analysis for the purposes of a specific national investigation; specific requests to the PIU with a view to PNR data analysis in response to a request for cooperation from a requesting competent authority; reception and forwarding of data to that authority; decisions relating to measures to be taken in the case of a positive analysis.

- **The allowed uses of the PNR database – in particular within the framework of proactive activities – must be clearly defined.**

The operations carried out on the PNR data fall into two processing categories.

Firstly, strategic analyses have to be carried out regarding the risks posed by certain passengers on certain flights. The operations which go into these analyses should be precisely defined, in particular on account of the legitimate questions raised by the concept of profiling. In this respect, it is worth pointing out that practitioners displayed a lack of interest in purely speculative searches such as those carried out for commercial purposes: they have neither the need nor the time to perform such searches.

The procedure for analysing the terrorist and criminal risk should be clearly delimited.

The analysis is primarily based on automated processing intended to help 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.

Furthermore, in the course of the many hearings organised, it emerged firstly that cross-analysis with API data (passport data) makes it possible to limit the risk of errors by enabling the identity of the persons in question to be checked, and secondly that it must be possible to supplement the risk analysis by cross-analysis with international, European or national files on persons or objects sought or under alert reported by the law-enforcement authorities (persons who are wanted or missing, minors who are not allowed to leave the country, stolen identification documents, etc.).

The air routes selected and processing operations to be carried out in the light of the risks identified should reflect needs as closely as possible. Accordingly, the strategic risk analysis must mainly be based on indicators drawn up by the competent departments, in a manner which is suited to the actual characteristics of the form of crime they are required to combat. At the same time, it is highly desirable to continue developing common methods and indicators within the EU in accordance with arrangements to be defined (see the customs experience).

Secondly, specific searches have to be carried out in response to specific queries submitted within the framework of investigations conducted by the competent authorities. In these cases, the analyses are carried out on the basis of the search criteria identified by these authorities. Only data relating to persons identified by the analyses are transmitted to these authorities by the PIU. Depending on the request, the data may relate both to a suspect and to other passengers who seem to have a link with that person (concept of "accompanying persons").

(e) Respect for fundamental rights/data protection

On the basis of the well-substantiated opinions issued by the competent European and national authorities, the need to include the following principles and rules can already be noted, in order firstly to clarify the applicable protection arrangements and secondly to adopt specific additional protection measures adapted to the nature of the PNR instrument.

- **The option of sole use of the push method can easily be retained**, while granting an adjustment period to airlines in order for them to bring their systems up to date.
- **The list of data to be transmitted can be reduced compared with the original proposal since it was not deemed necessary to maintain the information relating to unaccompanied minors which it contained.**
- **The protection arrangements applicable to the transmission of PNR data by airlines must be uniform**; national legislation should therefore provide for arrangements similar to those established for the transposition of Directive 95/46/EC for all processing of PNR data by airlines without distinction between commercial purposes and law-enforcement purposes.

- **Protection of data processed at national level must be aligned at the very least on the standards established by the Council of Europe:** each Member State must 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 must 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.

- **The Member States must provide for external supervision by independent authorities** (see Articles 11h and 11i of the current draft).

- **Exchanges of PNR data between Member States must comply with the rules of the Framework Decision on data protection** (currently being adopted and published). The importance of referring to that Framework Decision was stressed, in particular on account of the conditions which it lays down for forwarding data to third countries. These conditions would in fact be reproduced in the European instrument as regards exchanges of analytical data between a Member State and a third country.

- **A European PNR instrument should include clear rules to exclude arbitrary or discriminatory treatment.** The importance of ensuring human involvement in all decision-making processes and, accordingly, of prohibiting the taking of any decision liable to have negative consequences for someone solely on the basis of automated PNR data processing, must be highlighted. Obviously, no risk assessment criterion may be based on a person's race or ethnic origin, religious belief, political opinion, trade union membership, health or sexual orientation. Likewise, such elements may never be the starting-point for an investigation or search of any kind (see Articles 3(4), 4(6) and 11a of the current draft).

- The instrument should also provide for:

- **systematic verification by the PIU of the legality of the requests received**, before a reply is sent to the requesting authorities;
- **rigorous traceability of all access to the PNR database, all analyses and all transmissions made**;
- **erasure and rectification of inaccurate or incomplete data** (obligation regarding the means);
- **erasure of the results of risk analyses by the PIU** once they have been transmitted to the competent authorities, except where retention is justified in the interests of air passengers (elimination of "false positives");
- **establishment in each Member State of a system of appropriate sanctions** for use in the event of infringement of the data protection rules;
- **data security**: provision must be made for a robust system (see current Article 12 which can be supplemented by provisions ensuring sufficient securitisation of PIU premises);
- **informing air passengers of their rights of access, rectification, compensation and recourse** (see Articles 11c to 11g of the current draft instrument). The transparency of the instrument could be improved by adding two measures: informing the public by displaying notices in airports (information to be the responsibility of the public authorities and separate from the information already provided by airlines to their customers), and preparation of a European guide to passenger's rights of access.

(III) Main points outstanding

Proceedings must continue on the points not yet discussed or not discussed in sufficient detail. Many of them are listed in the outcomes of proceedings of the MDG meetings. The Presidency considers that three points on which discussions are in progress deserve to be cited in this report in view of their importance. The question of the transfer of data to third States should also be examined in greater detail.

(a) Sensitive data

Discussions have taken place on the question of the use of certain sensitive information which may be entered by the airline in a passenger's PNR file in order to improve his comfort on board and which may reveal religious adherence or health matters. It was pointed out that if the use of sensitive data were to be totally excluded, the obligation to erase could hardly be imposed on the air carriers without significantly increasing the technical and financial constraints on them. As practice now stands, such information cannot be processed automatically. Exclusion would therefore have to be based on individual erasure or blocking in the PIU.

It was pointed out that while the use of sensitive data is prohibited in principle, it is traditionally considered legitimate to allow reasoned use in a criminal investigation if the information it provides can either help solve the case or help exonerate the person concerned from all suspicion. If that approach were to be adopted for PNR, there would have to be a strict framework for the use of "sensitive" data.

(b) Retention period for data in the PIU

It has proved difficult to reach agreement on a figure for a harmonised retention period in the 27 Member States. The line proposed therefore is to set a compulsory data retention period sufficient to meet the needs of European cooperation, while setting a ceiling on the length of data retention authorised, in order to meet the data protection requirements.

On the basis of exploratory discussions in the MDG, it seems that the compulsory data retention period could easily be set at about 3 years, while the supplementary data retention period should be between 3 and 7 years. The total data retention period would thus be between 6 and 10 years.

(c) Exchange of bulk data

Detailed discussion of the particular issue of the exchange of bulk PNR data has begun and needs to be actively pursued. To begin with, the need for a clear definition of the notion of bulk PNR data has been recognised. The question is not so much the volume of data concerned but the fact that the data can be extracted from the PNR data base in "raw or semi-raw" state without any precise processing corresponding to any specific request. A very clear tendency has emerged to the effect that, as a general rule, such exchanges should take place only from one PIU to another within the framework of European cooperation.