Basic information

2007/0237(CNS) CNS - Consultation procedure Decision	Procedure lapsed or withdrawn
Use of passenger name record (PNR) for law enforcement purposes **Subject** 1.20.09 Protection of privacy and data protection 3.20.01.01 Air safety 7.30.20 Action to combat terrorism	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	IN 'T VELD Sophia (ALDE)	22/07/2009

Former committee responsible	Former rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs		

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	The committee decided not to give an opinion.	
TRAN Transport and Tourism	LICHTENBERGER Eva (Verts/ALE)	05/10/2009

Former committee for opinion	Former rapporteur for opinion	Appointed
AFET Foreign Affairs		
TRAN Transport and Tourism		

Council of the European Union

Council configuration	Meetings	Date
Justice and Home Affairs (JHA)	2899	2008-10-24
Justice and Home Affairs (JHA)	2887	2008-07-24
Justice and Home Affairs (JHA)	2908	2008-11-27

European Commission	

Commission DG	Commissioner
Justice and Consumers	BARROT Jacques

Key events

Date	Event	Reference	Summary
06/11/2007	Legislative proposal published	COM(2007)0654	Summary
11/12/2007	Committee referral announced in Parliament		
24/07/2008	Debate in Council		Summary
24/10/2008	Debate in Council		Summary
27/11/2008	Debate in Council		

Technical information

Procedure reference	2007/0237(CNS)
Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	Decision
Legal basis	Treaty on European Union (after Amsterdam) M 029 Treaty on European Union (after Amsterdam) M 034-p2b Treaty on European Union (after Amsterdam) M 030-p1
Stage reached in procedure	Procedure lapsed or withdrawn
Committee dossier	LIBE/7/00091

Documentation gateway

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2007)0654	06/11/2007	Summary
Document attached to the procedure	SEC(2007)1422	06/11/2007	
Document attached to the procedure	SEC(2007)1453	06/11/2007	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary

EDPS	Document attached to the procedure	52008XX0501(01) OJ C 110 01.05.2008, p. 0001	11/04/2008	Summary

Additional information		
Source	Document	Date
National parliaments	IPEX	
European Commission	EUR-Lex	

Use of passenger name record (PNR) for law enforcement purposes

2007/0237(CNS) - 11/04/2008 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

The Commission submitted the draft Framework Decision to the EDPS for an opinion. This proposal concerns the processing of PNR data within the EU and is closely related to other schemes of collection and use of passengers' data, in particular the EU-US agreement of July 2007. These schemes are of great interest to the EDPS, which considers that the present opinion should be mentioned in the preamble of the Council Decision.

The EDPS's opinion studies all aspects of the proposal but concentrates on the following elements which are considered to be fundamental:

1. **legitimacy of the proposed measures**: the question of the purpose, necessity and proportionality of the proposal are assessed against the criteria of Article 8 of the Charter of Fundamental Rights of the European Union;
2. **applicable law - exercise of data subject's rights**: the scope of application of the data protection framework decision in relation to the application of first pillar data protection legislation deserves specific attention;
3. **quality of recipients of data at national level**: in particular, the quality of Passenger Information Units (PIUs) of intermediaries and of competent authorities designated to perform risk assessment and analyse passenger data raises specific concerns as no precision is given in the proposal in this respect;
4. **conditions of transfer of data to third countries**: it is not clear what conditions will apply to such transfers where different sets of rules exist (the conditions of transfer under the present proposal, together with those of the data protection framework decision, and the existing international agreements with the USA and Canada).

With regard to the **legitimacy of the proposed measures**, the EDPS concludes that building upon different data bases without a global view on the concrete results and shortcomings is contrary to a rational legislative policy and might otherwise lead to a move towards a **total surveillance society**. Whilst the fight against terrorism can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection, the EDPS considers, however, that, to be valid, **the necessity of the intrusion must be supported by clear and undeniable elements**, and the proportionality of the processing must be demonstrated. This is all the more required in case of extensive intrusion in the privacy of individuals, as foreseen in the proposal. According to the EDPS, such elements of justification are missing in the proposal and that the necessity and proportionality tests are not fulfilled. The EDPS therefore insists on the **essential character of the necessity and proportionality** of the proposal which represent a *condicio sine qua non* to its entry into force.

With regard to the issue of the **applicable law and the exercise of this law by a person**, the EDPS considers that the proposal should make clear what legal regime is applicable at which stage of the processing, and specify vis-à-vis which actor or authority access and redress shall be exercised. He recalls that, according to the Treaty on European Union, provisions on data protection should be appropriate and cover the full range of processing operations established by the proposal. A simple reference to the data protection framework decision is not sufficient, given the limited scope of that framework decision and the restriction of rights it contains.

With regard to the **quality of recipients**, the EDPS considers that the enforcement of an EU PNR system is rendered even more difficult considering that law enforcement authorities have different competences depending on the national law of the Member States, including or not intelligence, tax, immigration or police. This is however a supplementary reason to recommend that the proposal be much more precise with regard to the quality of the mentioned actors and the guarantees to control the performance of their tasks. Additional provisions should be integrated in the proposal, to specify strictly the competences and the legal obligations of intermediaries, PIUs and other competent authorities.

Lastly, with regard to the **conditions of transfer to third countries**, the EDPS stresses the need to ensure that an adequate level of protection is provided in the recipient country. He also questions the significance of the 'reciprocity' principle mentioned in the proposal, and its application to countries already bound by an agreement with the EU, like Canada or the US. He considers it to be of the utmost importance that the conditions of transfer of PNR data to third countries be coherent and subject to a **harmonised level of protection**.

The EDPS also draws attention to specific aspects of the proposal that need more precision or a better taking into account of data protection principle (for example, the conditions in which automated decisions can be taken, the quantity of data processed, the method of transfer of data (or “push”), the data retention period, etc.).

Lastly, the EDPS notes that the present proposal is made at a moment when the institutional context of the European Union is about to change fundamentally. The consequences of the Lisbon Treaty in terms of decision making will be fundamental, especially with regard to the **role of the Parliament**. Considering the unprecedented impact of the proposal in terms of fundamental rights, the **EDPS advises not to adopt it under the present Treaty Framework, but to ensure it follows the co-decision procedure** foreseen by the new Treaty.

Use of passenger name record (PNR) for law enforcement purposes

2007/0237(CNS) - 06/11/2007 - Legislative proposal

PURPOSE: to fight terrorism and organised crime by obliging air carriers to transmit “Passenger Name Record” (PNR) data to the Member States’ competent authorities.

PROPOSED ACT: Council Framework Decision.

BACKGROUND: one of the EU’s core objectives is to offer its citizens a high level of security and protection within an area of freedom, security and justice. Terrorism and organised crime undermine and challenge this objective.

Studies prove that terrorism and organised crime are transnational in character and interlinked. The threat of terrorism is not restricted to specific geographic zones and terrorist organisations can be found both within and outside the border of the EU. For any measure against terrorism and organised crime to be effective a close cooperation and exchange of information between the Member States, competent authorities, Europol and third countries is essential. Critical to this is the collection of data, which for the purposes of this proposal, can be divided into two sets. Firstly, “Passenger Name Record” or PNR data. Specifically speaking PNR data refers to data collected from travel documents (usually flights). It includes: passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in flight schedule, seat preferences and other information. Air carriers already capture such data for their own commercial purposes.

The second set of data concerns “Advance Passenger Information” or API data, which essentially is biographical data. It includes: the number and type of travel document used, nationality, full names, date of birth, border crossing point of entry, code of transport, departure and arrival time of transportation, total number of passenger and the initial point of embarkation. API data may be run against alert systems such as the SIS. Under existing legislation, air carriers are obliged to communicate API data to the competent authorities of the Member States under Council Directive 2004/82/EC.

Given that API data is official data, stemming from passports, it is accurate. However, for the purpose of fighting terrorism and organised crime this information is useful only for identifying known terrorists and criminals through the alert system. It is not sufficient to help prevent terrorist acts or organised crime. PNR data, on the other hand, contains more elements. Further, it can be made available in advance of API data which is useful for carrying out risk assessments on persons, for obtaining intelligence and for making associations between known and unknown people.

Until now, only a limited number of Member States have adopted legislation obliging air carriers to provide the relevant PNR data to the competent authorities. Thus, the potential benefits of an EU wide scheme in preventing terrorism and organised crime is not being fully realised.

CONTENT: based on the above reasoning, the Commission is presenting this proposal the purpose of which is to oblige air carriers to transmit PNR data of international flights to the competent authorities of the Member States. The over riding objective is to prevent and combat terrorist offences and organised crime. It applies to air carriers only and to no other mode of transport. In summary, the following is being proposed:

- **Passenger Information Unit**: These are to be set up by the Member States within twelve months of the Decision entering into force. PIU’s will be responsible for collecting PNR data from the air carriers in relation to international flights which arrive or depart from the territory of the Member States which it serves. The Annex to the Decision gives a comprehensive list of all data required. Any data received and which is not specified in the Annex (i.e. ethnicity, political opinions, religious beliefs, trade union membership, health or sex life) must be deleted immediately. The PIU’s will be responsible for analysing data and for carrying out a risk assessment of the passengers in order to identify the persons requiring further examination. PNK data must be transferred to the relevant competent authorities within the other EU Member States by electronic means. Data may be processed on condition it is being used: to identify persons who are or who may be involved in a terrorist or organised crime offence; to create and update risk indicators; to provide intelligence on travel patterns; and/or to be used in criminal investigations and prosecutions of terrorist offences and organised crime. The PIU will be forbidden from taking any enforcement action based sole on an automated processing of PNR data.
- **Obligation on air carriers**: Air carriers will be responsible for making PNR data available to the PIU's by electronic means. The data must be made available in advance (24 hours before the scheduled flight departure) and immediately after flight closure. Data will be transmitted via the “push method” – i.e. data being transmitted from the air carriers to the national authorities. In cases where air carriers are unable to forward data to the competent authorities, the data can be extracted through the “pull method” – i.e. allowing the national authorities to access the reservation system of the air carrier.
- **Intermediaries**: Air carriers operating international flights may designate an intermediary who will be responsible for handling PNR data.
- **Exchange of information**: PNR data may only be transmitted to other EU Member States if it is deemed necessary to prevent and fight terrorism and organised crime. Procedures have been set concerning under what conditions requests for cross-border transmission of data may be made.

- **Data transfer to third countries**: PNR data may be transferred to third countries under two conditions: i) the Member State concerned is satisfied that the third country will only use the data to prevent and fight terrorist offences and organised crime and ii) the data will not be transferred further without the express consent of the Member State concerned.
- **Period of data retention**: Data must be kept for a period of five years after it has been transferred to the PIU. After the five year deadline air carriers must keep it for a further eight years – but it may only be accessed with the approval of the competent authority and only in exceptional circumstances (i.e. in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime.) Upon expiry of the eight year period all data will be deleted.
- **Sanctions**: The Member States will be responsible for sanctioning air lines that either do not transfer PNR data or transmit incomplete or erroneous data.
- **Protection of personal data**: The yet to be approved “Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters” will apply to the processing of personal data under this Decision. Member States will be responsible for security measures with respect to PNR data. Strict provisions are set out and include, inter alia, the physical protection of data; denying unauthorised persons access to the national installations; preventing unauthorised reading, copying, modification or removal of data media; preventing unauthorised inspection, modification or deletion of stored personal data; and preventing the unauthorised processing of data.
- **Comitology**: PNR data must be transmitted using secure methods common to all transmission. This will include common protocols and common encryption standards as adopted by the regulatory procedure. (One year after the common protocols have been adopted the Member States must apply the new secure method of transmission).

Use of passenger name record (PNR) for law enforcement purposes

2007/0237(CNS) - 24/07/2008

The Council held an exchange of views on the working method to be followed for the coming

months, and on a number of topics, in relation to the proposal for a Framework Decision on the use of passenger name records (PNR) by Member States' law-enforcement authorities.

Following the discussion, the Council confirmed its resolve to progress work on this proposal, involving partners such as the European Parliament, the personal data-control authorities and the Agency for Fundamental Rights.

It also agreed that work over the next few months should seek to gradually identify the essential features that the European PNR system should satisfy, on the basis of the following points in particular:

- priority to be given to the substance of the decision, with the legal basis being examined in the light of that substance;
- a balance to be sought between the need for a common tool and the flexibility which Member States may turn out to need;
- consideration based on operational use of data, which appears to be twofold: firstly in real time, resulting in action upon arrival of a flight, and secondly after the event, as part of investigations;
- examination of privacy protection in the light of the intended uses and with the incorporation of standards drawn up at European and national level;
- practical examination of technical arrangements for data collection, treatment of transit flights, the respective roles of passenger information units (PIUs) and relevant law-enforcement authorities, and the content of exchanges of information between PIUs.

The specific nature of the work to be carried out in the various areas in many cases makes it very helpful to bring into the discussions those with suitable technical competence. Involvement of the European Parliament in proceedings, by appropriate means, will also allow a constructive dialogue with that institution, which is particularly watchful as regards this proposal.

Since 9/11, law-enforcement authorities around the world have come to realise the added value of collecting and analysing so-called PNR data in combating terrorism and organised crime. PNR data are related to travel movements, usually flights, and include passport data, name, address, telephone numbers, travel agent, seat and other information. The PNR data of a certain passenger usually do not contain all PNR fields, but only those that are actually provided by the passenger at the time of the reservation and information received upon check-in and boarding. It must be noted that air carriers already capture the PNR data of passengers for their own commercial purposes, but that non-air carriers do not capture such data. The collection and analysis of PNR data allows the law enforcement authorities to identify high-risk persons and to take appropriate measures.

Use of passenger name record (PNR) for law enforcement purposes

2007/0237(CNS) - 24/10/2008

The Council discussed, **without yet reaching definitive conclusions**, some characteristics of a future passenger name record (PNR) system for collecting personal data gathered by air carriers when passengers book their tickets on international flights serving the territory of a Member State. The data, which would be forwarded to the public authorities before the passengers board the aircraft, would serve as input for analysing the terrorist and criminal threat and could also be used in the context of individual inquiries.

As regards including PNR data relating to intra-Community flights, the Council noted that the

cost-benefit ratio was an issue and that that point therefore needed to be assessed before deciding to include the data in the European instrument. The data are already being – and will continue to be – collected by some Member States at national discretion. The Council therefore agreed to review that specific issue once the PNR system had been in operation for a few years.

An overall report will be submitted to the JHA Council for endorsement at its next meeting on

27 and 28 November 2008. The Council will decide at that point on the follow-up to be given to that dossier.