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).