Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 14/04/2016 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 461 votes to 179 with 9 abstentions, a legislative resolution on the proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The position of the European Parliament adopted in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Purpose and scope: the purpose of the Directive is to ensure security, to protect the life and safety of the public, and to create a legal framework for the protection and exchange of PNR data between Member States and law enforcement authorities. It provides for:

- the **transfer by air carriers** of passenger name record (PNR) data of passengers of **extra-EU flights** ,
- the **processing of the data**, including its collection, use and retention by Member States and its exchange between Member States .

PNR data collected may be processed **only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime**.

Where an extra-EU flight has one or more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned.

If a **Member State decides to apply this Directive to intra-EU flights** (i.e. flying from one Member State to another Member States, without any stop-overs in the territory of a third country), it shall notify the Commission in writing.

Passenger information unit: each Member State shall establish an authority competent to act as its passenger information unit ('PIU'), responsible for:

- collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities;
- exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with **Europol**.

Data protection officer in the PIU: the PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards. A data subject must have the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject’s PNR data.

Processing of PNR data: the PIU may only process data for carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities, and, where relevant, by Europol, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

When carrying out this assessment, the PIU may: (i) **compare PNR data against databases** relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases ; or (ii) process PNR data against pre-determined criteria.

The data protection officer must have access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority. The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States.

The consequences of the assessments of passengers **shall not jeopardise the right of entry of persons enjoying the Union right of free movement** into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council.

Conditions for access to PNR data by Europol: the amended text states that Europol may submit, on a case-by-case basis, an electronic and **duly reasoned request to the PIU** of any Member State through the Europol National Unit for the transmission of specific PNR data or the result of processing those data. Europol may submit such a request 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.

Transfer of data to third countries: transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances and only if:(a) such transfers are essential to respond to a specific and actual threat related to terrorist offences or serious crime in a Member State or a third country, and (b) prior consent cannot be obtained in good time.

Period of data retention and depersonalisation: PNR data provided by the air carriers to the PIU must be retained in a database at the PIU for a **period of five years** after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.

Upon expiry of a period of **six months** after the transfer of the PNR data, all PNR data shall be **depersonalised through masking out the data elements which could serve to identify directly the passenger to whom the PNR data relate**, such as name, address and contact information, and all forms of payment information, including billing address, and frequent flyer information.

Upon expiry of the period of **six months**, disclosure of the full PNR data **shall be permitted only where** it is:(a) reasonably believed that it is necessary and (b) approved by either a judicial authority, or another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an ex-post review by that data protection officer.

Protection of personal data: the amended text states that the PIUs must maintain documentation relating to all processing systems and procedures under their responsibility. **Processing must not be based** on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. The PIU must keep **records** of at least the following processing operations: collection, consultation, disclosure and erasure. The records of consultation and

disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed the PNR data and the identity of recipients of those data. Those records shall be kept for a period of **five years**.

Review: the Commission shall conduct a review of all the elements of the Directive **four years** after the date of entry into force of the latter. It shall pay special attention to: compliance with the applicable standards of protection of personal data, the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, the length of the data retention period, and the effectiveness of exchange of information between Member States.