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

2011/0023(COD) - 07/09/2015 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the second report by Timothy KIRKHOPE (ECR, UK) 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 committee recommended that the position of the European Parliament adopted in first reading following the ordinary legislative procedure should amend 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. The Directive provides for the transfer **by air carriers and non-carrier economic operators**, such as travel agencies and tour operators, of Passenger Name Record data of passengers of **international flights to and from the Member States**, as well as the processing of that data, and its exchange between Member States and between the Member States and Europol.

Offences covered: the amended rules state that PNR data may be processed only for the purposes of prevention, detection, investigation and prosecution of **terrorist offences and of certain types of serious transnational crime.** The list approved by Members includes, for example, trafficking in human beings, child pornography, drug trafficking, trafficking in weapons, munitions and explosives, cybercrime and money laundering.

The definition of **terrorist offences** is taken from Council Framework Decision 2002/475/JHA, including individuals who may be travelling for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training.

Passenger Information Unit: the Unit shall be responsible for:

- collecting PNR data from air carriers and non-carrier economic operators, storing, processing and analysing those data and transmitting the result of the analysis to the competent authorities;
- the exchange of PNR data and of the result of the processing thereof with the Passenger Information Units of other Member States and with Europol.

Member States' Passenger Information Units would be entitled to process PNR data **only for limited purposes**, such as identifying a passenger who may be involved in a terrorist offence or serious transnational crime and who requires further examination. They would appoint a **data protection officer** to monitor data processing and safeguards and act as a single contact point for passengers with PNR data concerns.

Processing of PNR data: the application of the Directive must be duly justified and the **necessary safeguards** must be in place in order to ensure the lawfulness of any storage, analysis, transfer and use of PNR data.

In carrying out an assessment of the risk presented by a passenger, the Passenger Information Unit may **compare PNR data against the Schengen Information System and the Visa Information System.**

Passenger assessment criteria must be **targeted, specific, justified, proportionate and fact-based**. They must in no circumstances be based on person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sexual life.

Member States should also ensure that passengers are clearly and precisely informed about the **type of personal data** collected for law enforcement purposes and their rights.

Data retention period and masking out: PNR data transferred by air carriers and non-carriers would be retained in the national PIU for an initial period of 30 days, after which all data elements which could serve to identify a passenger would have to be **masked out**, and then for up to five years.

The masked out data would be accessible for up to **four years** in serious transnational crime cases and **five years** for terrorism ones.

After the five years, PNR data would have to be **permanently deleted**, unless the competent authorities are using it for specific criminal investigations or prosecutions (in which case the retention of data would be regulated by the national law of the Member State concerned).

Member States shall bear the costs of use, retention and exchange of PNR data. All data held by air carriers and non-carrier economic operators shall be held in a secure database on a **security accredited computer system** that either meets or exceeds international industrial standards.

Conditions for Europol to access PNR data: Europol may submit, on a case-by-case basis, an electronic and duly reasoned request to the Passenger Information Unit of any Member State for the transmission of specific PNR data or the results of the processing of specific PNR data, when this is strictly necessary to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious transnational crime.

Exchange of information shall take place by way of **SIENA** and in accordance with Decision 2009/371 /JHA.

Protection of personal data: the Passenger Information Units shall maintain: (i) **documentation** of all processing systems and procedures under their responsibility; (ii) ensure a **high level of securit**y appropriate to the risks represented by the processing and the nature of the PNR data to be protected; (iii) inform the person concerned by his or her **rights** and the arrangements for exercising these rights.

Passenger Information Unit must keep **records** of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The persons who operate security controls, access and analyse the PNR data, and operate the data logs, shall be **security cleared and security trained** .