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

2011/0023(COD) - 27/04/2016 - Final act

PURPOSE: to provide for the transfer by air carriers of PNR data and the processing of the data for the purposes of detecting, preventing, investigating and prosecuting terrorist offences and serious crime.

LEGISLATIVE ACT: Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

CONTENT: the Directive aims to **regulate the transfer to the EU, by air carriers, of passenger name record (PNR) data of passengers of extra-EU flights**, and the processing of such data by competent authorities.

If a Member State decides to apply the Directive to **intra-EU flights**, it shall notify the Commission in writing. A Member State may also decide to apply this Directive only to selected intra-EU flights. In making such a decision, the Member State shall select the flights it considers necessary in order to pursue the objectives of the Directive.

Passenger information unit (PIU): to ensure efficiency and a high level of data protection, Member States are required to ensure that an **independent national supervisory authority** and, in particular, a **data protection officer** are responsible for advising and monitoring the way PNR data are processed.

- 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.
- **The data protection officer** must have access to all data processed by the PIU, and if he considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority.
- **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.

Processing of data: PNR data gathered may only be used for the purposes of detecting, preventing, investigating and prosecuting terrorist offences and serious crime.

Accordingly, the PIU shall process PNR data only for carrying out an **assessment of passengers prior to their scheduled arrival in or departure** from the Member State. The assessment may only be carried out 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 the assessment, the PIU may: (a) compare PNR data against relevant databases; (b) process PNR data against **pre-determined criteria**.

Any assessment of passengers against pre-determined criteria shall be carried out in a **non-discriminatory** manner. Those pre-determined criteria must be targeted, proportionate and specific.

Transfer of data to third countries: a Member State may transfer PNR data to a third country, only on a case-by-case basis and in full compliance with the provisions laid down by Member States pursuant to Framework Decision 2008/977/JHA. Transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances.

Period of data retention and depersonalisation: the Directive provides for the retention of PNR data in the PIUs for a period of time **not exceeding five years**, after which the data should be deleted. It provides for the data to be depersonalised after an **initial period of six months**, through **masking out** of data elements which could serve to identify directly the passenger to whom the PNR data relate, such as name, address, and contact information, and also 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 under strictly defined circumstances.

Protection of personal data: all processing of PNR data should be **logged or documented** for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. The PIU must keep **records** of at least the following processing operations: collection, consultation, disclosure and erasure. Those records shall be kept for a period of **five years.**

The Directive **prohibits the processing of sensitive PNR data** revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.

Common protocols and supported data formats: as of one year after the date the Commission first adopts common protocols and supported data formats in accordance with paragraph 3, all transfers of PNR data by air carriers to the PIUs for the purposes of this Directive shall be made electronically using secure methods conforming to those common protocols.

ENTRY INTO FORCE: 24.5.2016.

TRANSPOSITION: 25.5.2018.