Use of passenger records to prevent terrorism and serious crime

SUMMARY OF:

Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

WHAT IS THE AIM OF THE DIRECTIVE?

- It aims to regulate the transfer of the passenger name record (PNR) data of passengers on international flights from airlines to the European Union (EU) countries.
- It also regulates the processing of these data by EU countries' competent authorities.

KEY POINTS

What are PNR data?

They consist of **booking information** stored by airlines in their reservation and departure control systems. The information collected includes:

- travel dates;
- travel itinerary;
- ticket information;
- contact details;
- means of payment used;
- baggage information.

Scope

- Each EU country must establish a **Passenger Information Unit** (PIU). A PIU is responsible for:
  - collecting, storing and processing the data, as well as transferring the data or the results of the processing to the competent national authorities;
  - exchanging PNR data and the results of processing with other EU countries and Europol.

Airlines must provide PIUs in EU countries with the PNR data for **flights entering or departing from the EU**. It also allows — but does not require — EU countries to collect PNR data concerning selected intra-EU flights.

Processing

The data collected may only be processed to **prevent, detect, investigate and prosecute terrorist offences and serious crime**. Data should only be processed in the following cases:

- for a pre-arrival assessment of passengers against pre-determined risk criteria and relevant law enforcement databases;
- for use in specific investigations/prosecutions;
- as input in the development of risk assessment criteria.

Transfer and exchange of data

- EU countries should not be able to access the database of airline companies.
- PNR data are sent by the airline to the PIU of the EU country concerned.
- When necessary and relevant, an EU country must supply PNR data on an identified person to the competent authorities of another EU country.
- PNR data may be transferred to a non-EU country under certain specific conditions.

Storage

- Data provided by airline carriers must be stored in a database by PIU for **5 years** from the time of its transfer to the EU country in which the flight is landing or departing.
- After **6 months** the transferred data must be **'depersonalised'** to mask out certain information including;
    - name;
    - address and contact information;
    - all payment information including billing address.
- Disclosure of the full PNR information after this 6-month period has expired is only permitted if:
    - it is reasonably believed to be necessary in order to respond to requests for PNR data made by competent authorities or Europol — on a case-by-case basis and;
    - it has been approved by a judicial or other national authority competent under national law to verify whether the conditions for disclosure are met.

FROM WHEN DOES THE DIRECTIVE APPLY?

The directive has applied since 24 May 2016. EU countries have to incorporate it into national law by 25 May 2018.

BACKGROUND

For more information, see:

- 'Passenger Name Record (PNR)' on the European Commission's website

MAIN DOCUMENT

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, pp. 132-149)