From day one, the Juncker Commission has made security a priority. Feeling safe and secure in your own home is a universal and basic right and Europeans rightly expect their Union to ensure this security. In the past 3 years, the Commission has been closing down the space in which criminals and terrorists operate: denying them the means to act and better exchanging information. The EU Passenger Name Record (PNR) Directive, which should be implemented by Member States by 25 May 2018, will help to track down travelling criminals and terrorists, closing an important information gap.

Criminals and terrorists increasingly operate across borders and their activities often involve international travel. Collecting and analysing PNR data from airlines will help to trace suspicious travel patterns, identifying potential criminals and terrorists, including those previously unknown to law-enforcement authorities.

Some Member States already use PNR data but the way this data is collected and shared varies from one Member State to another. The EU-wide PNR system, adopted on 27 April 2016, will harmonise different national laws: removing inconsistencies, plugging information gaps and ensuring a sufficient level of data protection and right to privacy. The new rules strictly limit the use of PNR data to the prevention, detection, investigation and prosecution of serious crime and terrorism. Under the EU PNR rules, participating Member States are required to set up a legal and technical framework for the transfer, processing and exchange of PNR data provided by airlines.

The deadline for incorporating the new EU PNR rules into national law is 25 May 2018.

WHAT IS PNR DATA?

Passenger name record (PNR) data, stored in airlines’ reservation systems, is information that is provided by passengers to airlines when booking flights and checking-in for flights. It includes information such as the passenger’s name, travel dates, travel itineraries, seat number, baggage, contact details and means of payment.

The EU PNR Directive will not require airlines to collect or retain any further data than that which is already collected for commercial purposes.

PARTICIPATING COUNTRIES

27 Member States*

*Denmark is not participating.
HOW DOES IT WORK?

1. When booking their flights, passengers provide airlines or travel agents with basic information such as contact details and means of payment.

2. This PNR data provided by passengers and collected by airlines and travel agents for passengers on international flights entering or departing from the EU will be transferred to dedicated Passenger Information Units (PIUs) in the respective EU Member State.

3. The PIUs will then analyse the PNR data in order to identify high-risk passengers, including previously unknown persons, prior to their arrival or departure, to detect suspicious travel patterns or facilitate the investigation, prosecution, and unravelling of criminal networks.

4. PNR data can be exchanged with Member State authorities or requested by Europol for law-enforcement purposes only.

The new PNR rules also allow Member States to collect PNR data concerning intra-EU flights.

WHAT WILL CHANGE FOR TRAVELLERS?

- The new rules do not carry additional burdens for travellers. They will be informed that their data is being collected but will not have to provide any more information than usual when booking their flights.

STRONG PROTECTION OF PRIVACY AND PERSONAL DATA

- Processing of PNR data must ensure full respect for data protection standards and other fundamental rights.
- The PNR Directive requires specific safeguards for processing of personal PNR data. PNR data may only be used for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
- Collection and use of sensitive data, such as those revealing a passenger's race or ethnic origin, religion or state of health, is prohibited.
- PNR data must be anonymised after 6 months, and deleted after 5 years.
- All PIUs in EU Member States are monitored by an independent national supervisory authority that oversees the processing of PNR data.
- All national PIUs are obliged to have a Data Protection Officer.