

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

2011/0023(COD) - 26/04/2012 - \${summary.subTitle}

The Council agreed a general approach on a draft directive on the use of flight passenger data for protection against terrorist offences and serious crime (PNR data). The agreement among Member States on a general approach allows the Danish presidency to start negotiations with the European Parliament under the ordinary legislative procedure.

The discussion in the Council touched, among other things, on two main issues:

- 1) The first question concerned whether the proposed new rules should be limited to the collection of the Passenger Name Record (PNR) data for flights from and to third countries or whether flights within the EU should also be covered. The proposed compromise would allow, but not oblige, Member States to collect PNR data also concerning selected intra-EU flights.
- 2) The second question discussed was the retention period. The initial Commission proposal provides for a total retention period of five years. After 30 days, however, the PNR data would have to be masked out, so that the person-related elements of the PNR were no longer visible to the "front-desk" law enforcement officer, but can be seen only after a specific authorisation. A number of Member States considers that this initial storage period of 30 days is too short from an operational point of view. The Council position agreed upon now is to maintain the overall retention period of five years but to prolong the first period during which the data are fully accessible to two years.

The Council also adopted a [decision on the conclusion of a new EU-US PNR agreement](#) which will replace the existing one, provisionally applied since 2007. The European Parliament had given its consent on 19 April 2012. The agreement is expected to enter into force on 1 June 2012.

The aim of the agreement is to set up a legal framework for the transfer of PNR data by carriers operating passenger flights between the European Union and the United States to the US Department of Homeland Security (DHS) and the subsequent use of that data by the US DHS. The goal is to prevent, detect, investigate and prosecute terrorist offenses and related crimes as well as other serious cross-border crimes punishable by a sentence of imprisonment of at least three years.

The main aspects of the new PNR agreement with the US are:

- a strict purpose limitation, the use of PNR data being limited to the prevention, detection, investigation and prosecution of terrorist offences or transnational crime;
- a legally binding commitment from the US Department of Homeland Security to inform the Member States and EU authorities of any EU relevant intelligence leads flowing from the analysis of these PNR data;
- a robust data protection regime with strong data security and integrity requirements;
- rights of access, rectification and erasure and the possibility to obtain administrative and judicial redress;
- a limited usage of PNR data for a period of ten years for transnational crime and 15 years for terrorism. After 6 months personally identifiable information of PNR data will be masked out and after five years PNR data will be moved to a dormant database with additional controls.