European Parliament

# Completing the adoption of an EU PNR Directive

The compromise text on the long-debated proposal for an EU PNR (Passenger Name Records) Directive is now due to be voted in plenary in April. It aims at uniformly regulating the processing and sharing of passenger name records by Member States in the fight against terrorism and serious crimes, while putting in place a series of data protection safeguards.

## A long path

The adoption of a common EU PNR system as part of the European security strategy has long been debated: the European Commission proposed a directive in 2011 (following an earlier proposal in 2007) on which the Council reached a general approach in 2012. However the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) rejected it in 2013, questioning its necessity and proportionality. Following the early 2015 Paris attacks and subsequent calls for an EU PNR scheme from different quarters (such as the European Council and the EU Counter-terrorism Coordinator), the proposal gained momentum again, as a means to counter the phenomenon of foreign fighters. After several debates on a revised report presented in February by rapporteur Timothy Kirkhope (ECR, UK), on 15 July the Committee adopted a second report, enabling the opening of negotiations with the Council. The November Paris attacks gave impetus to a compromise, subsequently endorsed by the Council and backed by LIBE in December2015.

## Counter-terrorism policy

PNR data consist of information on air passengers held by air carriers for operational purposes, such as passengers' names, travel dates, itinerary and payment method. PNR data are already collected by law enforcement bodies for security purposes in some Member States (UK and Denmark). Under the proposed directive, which seeks to harmonise rules for the use of such data, airlines will be obliged to transfer ('push') PNR data of passengers of extra-EU flights to the Member State in which a flight will land or from which it will depart. Each Member State will designate a Passenger Information Unit (PIU) to store and assess PNR data (mainly comparing PNR of unsuspected persons against databases), in order to *identify persons requiring further examination by the competent authorities* to which PNR are then transmitted on a case by case basis. PNR data are to be retained for five years: all identifying data fully available for six months, then stored in a masked format (initially the Commission proposed 30 days, the Council two years). PIUs will also exchange information among Member States, as law enforcement authorities will not have direct access to airline data systems ('pull'). The collection and use of sensitive data (revealing racial origin, religion, political opinion, health or sexual orientation) should be prohibited. The compromise text includes the *possibility* for a Member State to apply the directive to intra-EU flights, as proposed by the Council; in this case it must notify the Commission. Member States may also collect PNR data from travel agencies and tour operators.

## Data protection

The EP has consistently sought to make the directive compliant with the proportionality principle, and to include data protection (DP) safeguards, such as a narrow list of serious crimes justifying the use of PNR; the appointment of DP officers in each PIU; the strengthening of DP authorities' monitoring powers; and strict conditions to access masked PNR data beyond six months. In a resolution on anti-terrorism measures, the EP, while committing to finalising the EU PNR scheme, urged the co-legislators to advance trilogues on the Data Protection Package, in parallel. The aim was to align the related provisions, also in view of recent CJEU case law. This position was reiterated in later resolutions on the European Agenda on security and on prevention of radicalisation. In his second opinion on the directive, the European Data Protection Supervisor urged strict safeguards against the risk of mass surveillance, such as limiting the use of PNR data to concrete security threats, as well as its retention period and access to it by competent authorities.

EPRS | European Parliamentary Research Service
Author: Shara Monteleone, **Members' Research Service**
PE 580.886