

Dods EU Alert

Source: European Parliament Press Release

Subject: EU Passenger Name Record (PNR): Civil Liberties Committee backs EP/Council deal

Date published: December 10 2015

The provisional deal reached by Parliament and Council negotiators last week on an EU directive regulating the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was endorsed by the Civil Liberties, Justice and Home Affairs Committee on Thursday by 38 votes to 19, with 2 abstentions. The draft directive will be put to a vote by Parliament as a whole early next year.

"We cannot wait any longer to put this system in place. (...) The choice is not between an EU PNR system and no EU PNR system; it is between an EU PNR system and 28 national PNR systems that will have vastly differing, or absent, standards for protecting passenger data", said Parliament's Civil Liberties Committee lead negotiator on the EU PNR proposal, Timothy Kirkhope (ECR, UK).

The EU PNR directive would oblige airlines to hand EU countries their passengers' data in order to help the authorities to fight terrorism and serious crime. MEPs sought to ensure, in three-way talks ("trilogues") with the Council and Commission, that the draft law complies with the proportionality principle and includes strict personal data protection safeguards.

PNR data is information provided by passengers and collected by air carriers during reservation and check-in procedures, such as travel dates, travel itinerary, ticket information, contact details, baggage information, payment information, etc.

Flights included in the scope

The agreed directive will provide for the transfer by air carriers to EU member states' "Passenger Information Units" (PIUs) of PNR data of passengers of "extra-EU flights" (i.e. from a third country to an EU member state or vice-versa). It will allow, but not oblige, member states to apply its provisions also to "intra-EU flights" (i.e. from an EU member state to one or more of the other). If a member state wishes to apply this directive to intra-EU flights, "it shall give notice in writing to the Commission to that end", says the text.

Non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services including booking flights, for which they collect and process PNR data, are not included in the directive's scope, but it does allow member states to provide, under their domestic law, for a system for collecting and processing PNR data from these operators.

The PNR data may be processed "only for the purposes of prevention, detection, investigation and prosecution of terrorist offences and serious crime". A single list of offences has been agreed upon, including, for example, trafficking in human beings, participation in a criminal organisation, cybercrime, child pornography, and trafficking in weapons, munitions and explosives.

Data retention and "masking out"

The PNR data provided by the air carriers to the national PIUs is to be retained for a period of five years. For the first six months, the data will be "unmasked", i.e. will include personal identifying information. The data will then have to be "masked out" for the remaining four and a half years.

Depersonalising data through "masking out" means rendering certain data elements of such data invisible to a user, such as name(s), including the names of other passengers on PNR and number of travellers on PNR travelling together, address and contact information, etc. (i.e. data elements which could serve to directly identify the passenger to whom the PNR data relate).

At the insistence of the Parliament's lead negotiator, the initial storage period during which the PNR data are not "masked out" is six months (the Council's general approach sought to prolong the first period during which the data are fully accessible to two years, from the 30 days in the initial Commission proposal presented in 2011).

Extra data protection safeguards

Data protection safeguards inserted by MEPs during the negotiations include:

- an obligation for national PIUs to appoint a data protection officer responsible for monitoring the processing of PNR data and implementing the related safeguards, and to act as a single point of contact on all issues relating to the processing of the passengers' PNR data,
- duties and powers for the national supervisory authority, which will be in charge of checking the lawfulness of the data processing and conduct investigations, and
- access to the full PNR data set, which enables users to immediately identify the data subject, should be granted only under very strict and limited conditions after the initial retention period.

All processing of PNR data should be logged or documented, and passengers should be clearly and precisely informed about the collection of PNR data and their rights.

Review clause

At MEPs' request, the agreed text requires the Commission to carry out a review of the EU PNR directive two years after its transposition into national laws. It must pay special attention to compliance with personal data protection standards, the necessity and proportionality of collecting and processing PNR data for each of the stated purposes, the length of the data retention period, and also "the effectiveness of the sharing of data between the member states". The necessity of introducing non-carrier economic operators within the scope of the directive should also be looked at during the review process, says the agreed text.

In the light of this review, a proposal to amend the EU PNR directive could be presented.

Next steps

The draft directive is to be put to a vote by Parliament as a whole early in 2016 and then formally approved by the EU Council of Ministers. Member states will have to transpose the EU PNR directive into their national laws at the latest two years after its entry into force.

The UK and Ireland have opted in to this directive, while Denmark has a "blanket" opt-out for justice and home affairs legislation.