IP/10/1150

Brussels, 21 September 2010

European Commission adopts an EU external strategy on Passenger Name Record (PNR)

The European Commission adopted today a package of proposals on the exchange of Passenger Name Record (PNR) data with third countries, consisting of an EU external PNR strategy and recommendations for negotiating directives for new PNR agreements with the United States, Australia and Canada.

"In this strategy, we set the general principles that any PNR agreement with a third country should be based on. PNR data has proven to be an important tool in the fight against serious transnational crime and terrorism, but at the same time, it raises important issues about protection of personal data", said EU Commissioner for Home Affairs Cecilia Malmström.

More and more third countries use Passenger Name Record (PNR) data in the fight against terrorism and serious transnational crime. Law enforcement authorities can use data provided by a passenger to book a flight to investigate past crimes, prevent new ones and make risk analysis.

Currently the exchange of PNR data with third countries is done under different frameworks. Continuing this situation when PNR data is an increasingly popular security tool, would adversely affect legal certainty and the protection of passengers' personal data.

The Communication presented today sets general principles that any PNR agreement with a third country should observe:

1. Protection of personal data, which aim to protect the rights of passengers:

- PNR data should be used exclusively to fight terrorism and serious transnational crime.
- The categories of the PNR data exchanged should be limited to what is necessary for that purpose, and be clearly listed in the agreement.
- Passengers should be given clear information about the exchange of their PNR data, have the right to see their PNR data and the right to effective administrative and judicial redress. This helps ensure full respect for privacy and that any violation of privacy will be remedied.
- Decisions having adverse effects on passengers must never be based on an automated processing of PNR data. A human being must be involved before a passenger is denied boarding. This seeks to prevent "profiling".
- Third countries must ensure a high level of data security and an effective independent oversight of the authorities which use PNR data.
- The PNR data cannot be stored longer than necessary to fight terrorism and serious transnational crime, and third countries should limit who has access to the data gradually during the period of retention.

- PNR data may be shared by the third country with other countries (onward transfer) only if those countries respect the standards laid down in the PNR agreement between the EU with the third country, and only on a case-by-case basis.

2. Modalities of transfer of the PNR data, which aim to provide legal certainty to air carriers and keep costs at an acceptable level: PNR data should be transmitted using the "PUSH" system, and the number of times that data is transferred before each flight be limited and proportionate.

3. Standards on monitoring the correct implementation of the PNR agreement, for instance on review, monitoring, effective dispute resolution.

4. Reciprocity should also be ensured. Information about terrorism and serious transnational crime resulting from the analysis of PNR data by third countries should be shared with EUROPOL, EUROJUST and EU Member States.

For more information

Homepage of Cecilia Malmström, EU Commissioner for Home Affairs:

http://ec.europa.eu/commission_2010-2014/malmstrom/index_en.htm

MEMO/10/431