

EU/USA Agreement: use and transfer of passenger name records (PNR) to the US Department of Homeland Security

2011/0382(NLE) - 19/01/2017 - Follow-up document

The Commission presented a report on the joint review of the implementation of the Agreement between the United States of America and the European Union on the use of Passenger Name Record (PNR) data and their Transfer to the US Department of Homeland Security.

The current agreement between the United States of America and the European Union on the use of passenger name record (PNR) data and their transfer to the US Department of Homeland Security (DHS) came into effect on 1 July 2012.

The main purpose of the joint review is to report on the follow-up to the recommendations of the previous report of 2013 and the implementation of the agreement, paying particular attention to the mode of transmission of PNR data and the subsequent transfer of such data as provided for in the relevant articles of the agreement.

The report also outlines the main findings of the 2015 joint review and the issues that still remain to be addressed by the DHS.

Implementation of the 2013 recommendations: the Commission considers that all the recommendations made following the 2013 review have either been fully respected or followed up by further improvements:

- **internal privacy review:** the launch of the six-month period, triggering the depersonalisation of PNR data under the agreement now starts on the date when PNR data are loaded into the automated targeting system (ATS) (known as the “load date”), which is the first day the data are stored in the system;
- **full move to the “push” method by 1 July 2014:** during the 2015 review, four air carriers still did not communicate PNR data using the "push" method; The DHS helped them develop their capacity to do so;
- **notification procedure to EU Member States in the event of sharing of EU PNR data between DHS and third countries:** since July 2014 a Customs and Border Protection (CBP) officer has been seconded to Europol as liaison officer. Where the liaison officer identifies a "targeted" passenger with a link to a Member State, he shares the information with the representatives of that Member State in a report;
- **transparency in the remedies available to individuals:** the DHS's TRS (Traveler Redress Inquiry Program) is the single point of contact for the public, but the United States should continue to examine all means to ensure that all passengers are informed of the available redress mechanisms.

Recommendations following the 2015 review: The EU Task Force noted that the United States continued to implement the agreement in accordance with the conditions set out therein:

- the DHS complies with its obligations as regards access rights for passengers and has a monitoring mechanism to prevent unlawful discrimination;
- constant efforts have been made to ensure reciprocity and preventive sharing of analytical information derived from PNR data with Member States and, as appropriate, with Europol and Eurojust;
-

- the masking and deletion of sensitive data is respected and the DHS has stated that it has never had access to sensitive data for operational purposes;
- the DHS continues to honour its commitments on passenger rights, in particular with respect to the provision of passenger information and the implementation of the right of access without any derogation;
- data sharing with other US services is handled by the DHS in accordance with the agreement. It is done on a case-by-case basis, is recorded and takes place on the basis of written agreements. The sharing of data with third countries is strictly interpreted and is also in line with the agreement.

Opportunities for improvement: despite the successful implementation of the agreement, some improvements remain necessary:

- the number of overrides to access non-US nexus PNR data has increased since the 2013 review and the DHS needs to record the reasons why overrides have been used to better understand why they occur;
- the DHS should continue to monitor the number of officers with access rights to PNR data in order to limit the consultation and use of PNR data only to staff with an operational need to do so;
- the DHS should regularly monitor the list of sensitive data codes in order to ensure that all sensitive data are automatically blocked by the system;
- the number of PNR data related to repressive operations and therefore not subject to masking remains high. The DHS is invited to examine this point and to ensure that the data in question no longer need to be hidden, anonymised or deleted as soon as possible;
- the DHS complies with the agreement by not refusing any passenger access to their data. However, response times have increased since the last review in 2013 and the DHS should establish whether it is possible to reduce them;
- the DHS should provide more information on the precise data currently being collected and be able to provide more information on data that has been shared with other US authorities and police, law enforcement and judicial bodies within the EU;
- lastly, with a view to future reviews and evaluation, the DHS should ensure that all facts and figures are collected in a uniform manner to allow for direct comparisons.