Press release

Civil Liberties Committee green light for air passenger data deal with the US

Committees: Committee on Civil Liberties, Justice and Home Affairs

A new agreement on the transfer of EU air passengers' personal data to the US Department of Homeland Security was approved by the Civil Liberties Committee on Tuesday. The deal sets the legal conditions for the transfer of this data and covers issues such as storage periods, purpose of the data use, data protection safeguards and administrative and judicial redress. The agreement is intended to replace another deal applied provisionally since 2007.

Passenger Name Record (PNR) data are collected by air carriers during the reservation process and include, inter alia, names, addresses, credit card details and seat numbers of air passengers. Under US law, air companies are obliged to make these data available to the Department of Homeland Security (DHS) prior to passenger departure. This applies to flights to or from the US.

The EU-US PNR deal was approved with 31 votes in favour, 23 against and one abstention. The EPP and ECR groups voted in favour. In a debate last February, a number of MEPs said that it was better to have an agreement, albeit not entirely satisfactory, than to have no agreement at all. The ALDE, Greens/EFA and GUE/NGL groups voted against, because they consider that data protection safeguards foreseen in the agreement do not meet EU standards. S&D MEPs were split.

Following the vote, rapporteur Sophie in'T Veld (ALDE, NL) explained: "The results of the vote show clearly that there are very strong reservations against this agreement. However, the US made it very clear that a "no" vote would be answered by suspending visa-free travel to the US. Many colleagues - understandably - did not want to make this sacrifice. But it is highly regrettable that the fundamental rights of EU citizens have been bargained away under pressure".

Retention period and purpose

Under the new agreement, PNR data would be retained by the US authorities in an active data base for up to 5 years. After the first 6 months, all information which could be used to identify a passenger would be "depersonalized", meaning that data such as the passenger's name or her/his contact information would be masked out.

After the first 5 years, the data would be moved to a "dormant database" for up to 10 years, with stricter access requirements for US officials. Thereafter, the agreement says, data would be fully "anonymized" by deleting all information which could serve to identify the passenger. Data related to any specific case would be retained in an active PNR database until the investigation is archived.

PNR data would be used mainly to prevent, detect, investigate and prosecute terrorism and serious transnational crimes. Transnational crimes are defined as crimes punishable by 3 years of imprisonment or more under US law. PNR data can also be used case by case in the event of a serious threat or if ordered by a US court. The agreement negotiated by the Commission in 2011 says that PNR data could also serve "to identify persons who would be subject to closer questioning or examination".

Press Service
Directorate for the Media
Director - Spokesperson : Jaume DUCH GUILLOT
Reference No:20120326IPR41838
Press switchboard number (32-2) 28 33000

Sensitive data and "push-pull"

Sensitive data such as those revealing the racial or ethnic origin, political opinions, religious beliefs, physical or mental health or sexual orientation of a passenger could be used in exceptional circumstances when a person's life is at risk. This data is most frequently tied to a religious meal choice or requests for assistance due to a medical condition. This data would be accessed only case-by-case and would be permanently deleted after 30 days from receipt, unless it is used for a specific investigation.

Within 2 years of the agreement's entry into force, all air companies would be required to transfer PNR data to the DHS using the "push" method, meaning that carriers send the data themselves. However, in certain cases, if a company is unable for technical reasons to send the data timely, the US authorities could require access to the carrier's data system ("pull" method).

Data protection and judicial redress

To prevent any accidental loss or unauthorised disclosure of data, PNR would be held in a secure environment protected with physical intrusion controls. Should their data be misused, EU citizens would have the right to administrative and judicial redress in the US. They would also have the right to access their own PNR data and seek rectification by the DHS, including the possibility of erasure, if the information is inaccurate.

Next steps

The agreement will be put to a plenary vote on 19 April. If Parliament gives its consent, the Council will adopt a decision concluding the agreement, which would then be in force for seven years. If approved, the new agreement would replace the current one, which has applied provisionally since 2007.

If Parliament as a whole rejects the 2011 PNR agreement, the 2007 deal would continue to apply provisionally (its expiry date is July 2014). In May 2010, Parliament postponed its vote on the 2007 agreement and called on the Commission to negotiate a new text. So if the 2011 deal is rejected, Parliament might have to vote on the 2007 deal too.

Background

The European Parliament adopted in October 2011 a deal with Australia on the processing and transfer of PNR data. The EU is currently negotiating a new PNR agreement with Canada.

27.03.2012
In the chair: Juan Fernando López Aguilar (S&D, ES)
Procedure: consent
Plenary vote: 19.04.2012

Contact :

Natalia DASILVA
BXL: (+32) 2 28 44301
STR: (+33) 3 881 73661
PORT: (+32) 498 98 39 85
EMAIL: libe-press@europarl.europa.eu