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

2011/0382(NLE) - 09/12/2011 - Document attached to the procedure

Opinion of the European Data Protection Supervisor (EDPS) on the proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security

On 28 November 2011, the Commission adopted a proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security. On 9 November 2011, the EDPS was consulted informally on the draft proposal, in the context of a fast track procedure. On 11 November 2011, he issued a number of restricted comments. The aim of the present Opinion is to complement these comments in light of the present proposal and to make his views publicly available.

Background to the proposal: the agreement aims at providing a solid legal basis for the transfer of PNR data from the EU to the US. The transfer is currently based on the 2007 agreement because the Parliament decided to postpone its vote on the consent until its data protection concerns were met. In particular, in its resolution of 5 May 2010, the Parliament referred to the following requirements:

- compliance with data protection legislation at national and European level,
- a privacy impact assessment prior to the adoption of any legislative instrument,
- a proportionality test demonstrating that existing legal instruments are not sufficient,
- strict purpose limitation and limitation of the use of PNR data to specific crimes or threats, on a case-by-case basis,
- limitation of the amount of data to be collected,
- limited retention periods,
- prohibition of data mining or profiling,
- prohibition of automated decisions significantly affecting citizens,
- appropriate mechanisms for independent review, judicial oversight and democratic control,
- all international transfers should comply with EU data protection standards and be subject to an adequacy finding.

The present agreement must be considered in the context of the global approach to PNR, which includes negotiations with other third countries (namely Australia and Canada, and a proposal for a PNR scheme at the EU level. It also falls within the scope of the current negotiations for an agreement between the EU and the US on the exchange of personal data in the framework of police and judicial cooperation in criminal matters. In a wider context, the agreement has been initialled a few weeks before the expected adoption of the proposals for the review of the general data protection framework.

Main observations:

The EDPS welcomes the safeguards on data security and oversight provided for in the agreement and the improvement compared with the 2007 agreement. Nevertheless, various concerns persist, particularly as regards:

- the consistency of the overall approach to the question of PNR data,
- the purpose limitation,
- the list of data to be transferred to the DHS,
- the processing of sensitive information,
- the exceptions to the "push" method,
- the rights of persons concerned and subsequent transfers of the data.

Consistency of the approach: while this agreement includes some improvements in comparison with the 2007 agreement, and includes adequate safeguards on data security and oversight, **none of the main concerns expressed in the European Parliament's resolution were met.**

Purpose: although the definitions are more precise than in the 2007 agreement, there are still some vague concepts and exceptions that could override the purpose limitation and undermine legal certainty. In particular, the EDPS mentions:

- the lack of precision in the list 'other crimes that are punishable by a sentence of imprisonment of three years of more' as this threshold includes different crimes in the EU and the US and in the different EU Member States and US States; moreover, minor offences should be explicitly excluded from the purpose of the agreement;
- the concept of 'serious threat' should be defined and the use of PNR data where 'ordered by a court' should be limited to very specific cases.

List of PNR data to be transferred: this list should be narrowed: Annex I of the agreement contains 19 types of data that will be sent to the US. While assessing the proportionality of the list, it should also be taken into account that, due to advanced transmission, these categories will refer not only to actual passengers but also to those individuals who do not finally fly (e.g. due to cancellations). This is why the EDPS considers that data should be limited to the following information:

- PNR record locator code,
- date of reservation,
- date(s) of intended travel,
- passenger name,
- other names on PNR,
- all travel itinerary,
- identifiers for free tickets,
- one-way tickets,
- ticketing field information,
- ATFQ (Automatic Ticket Fare Quote) data,
- ticket number,
- date of ticket issuance,
- no show history,
- number of bags,
- bag tag numbers,
- go show information,
- number of bags on each segment,
- voluntary/involuntary upgrades,
- historical changes to PNR data.

DHS should not process sensitive data: Article 6 of the agreement states that the DHS shall automatically filter and 'mask out' sensitive data. However, sensitive data will be stored **at least 30 days** and might be used in specific cases. The EDPS would stress that even after being 'masked out', these data will still be 'sensitive' and relate to identifiable natural persons and should therefore **not be processed by the DHS**.

The data retention period: Article 8 states that PNR data will be retained for up to **five years** in an active database and then transferred to a dormant database and stored for up to **10 years**. This maximum retention period of 15 years is clearly disproportionate, irrespective of whether the data are kept in 'active' or 'dormant' databases.

Use of the 'push' method and frequency of the transfers: the EDPS welcomes Article 15(1), which states that data will be transferred using the 'push' method. However, Article 15(5) requires carriers to 'provide access' to PNR data in **exceptional circumstances**. In order to definitively preclude the use of the 'pull' system, the EDPS strongly advises that the agreement expressly prohibits the possibility for US officials to separately access the data via a 'pull' system.

Data security: although the EDPS welcomes Article 5 of the agreement on data security and integrity, certain aspects are problematic and, in particular, the recipients of the notification, who should be specified. The EDPS strongly supports the right to redress 'regardless of nationality, country of origin, or place of residence' laid down in Article 14(1), second subparagraph. However, he regrets that Article 21 explicitly states that the agreement 'shall not create or confer, under US law, any right or benefit on any person'. Even if a right to 'judicial review' is granted in the US under the agreement, such right may not be equivalent to the right to effective judicial redress in the EU, in particular in the light of the restriction stated in Article 21.

Onward national and international transfers: the agreement prohibits the transfer of the data to domestic authorities that do not afford to PNR 'equivalent or comparable' safeguards to those set forth in this agreement. The EDPS welcomes this provision. The list of authorities that might receive PNR data should however be further specified.

As regards international transfers, the agreement provides that they should only take place if the recipient's intended use is consistent with this agreement and adduces privacy safeguards 'comparable' to the ones provided in the agreement, except in emergency circumstances.

With regard to the wording 'comparable' or 'equivalent' used in the agreement, the EDPS would like to emphasise that **no domestic or international onward transfers** by the DHS should take place unless the recipient adduces safeguards that are not less stringent than the ones established in this agreement. It should also be clarified in the agreement that the transfer of PNR data shall be done on a case-by-case basis, ensuring that only the necessary data will be transferred to the relevant recipients, and no exceptions should be allowed. In addition, the EDPS recommends that data transfers to third countries should be subject to prior judicial authorisation.

Article 17(4) states that when data of a resident of an EU Member State are transferred to a third country, the competent authorities of the Member State concerned should be informed in cases where the DHS is aware of this situation. This condition should be deleted, as the DHS should **always** be aware of onward transfers to third countries.

Form and review of the agreement: lastly, the EDPS considers that the legal form chosen by the US for entering into this agreement and how this agreement will become legally binding in the US should be clarified. The agreement should also be reviewed in view of the new data protection framework and of the possible conclusion of a general agreement between the EU and the US on the exchange of personal data in the framework of police and judicial cooperation in criminal matters. A new provision should be added to this effect.