Is the new EU-US PNR Agreement acceptable?

The European Parliament will have to vote soon on an Agreement for the transfer to the US, subsequent use and retention of European citizens' data (PNR) travelling to the US. However, the proposed Agreement is still deeply flawed. In its Resolutions of 5 May 2010 and 11 November 2010, the European Parliament raised serious concerns about the upcoming negotiations and the general approach to transfers of passenger name record (PNR) data to third countries. The current proposal has not addressed any of the demands and flaws identified by the European Parliament. The criteria set in its Resolutions are not met.

Among the wide range of problems of the current proposal, these are, we believe, the most important questions:

1. Has the retention period been reduced?

No. The European Parliament asked for a limitation of the length of storage periods[1], but the new Agreement would allow a storage period of 15 years. According to Article 8, data are retained in an active database for up to 5 years and then transferred to a dormant database for a period of up to 10 years. As the Article 29 Working Group highlights, this still means that the "data of unsuspected citizens is stored for up to 15 years, only its use would be more limited".[2]

The Commission has neither provided evidence that the collection, storage and processing of personal data is proportionate at all, let alone why it appears to believe that 15 years of data retention are necessary and proportionate.

2. Is there a meaningful anonymisation of the data after 6 months?

No. The Agreement would only require that the DHS copies of PNR data be "depersonalized" after six months. This means that while some data fields are not accessible to every official involved in the PNR data usage, but for others, the data will still be accessible with full personalisation. Even worse: The data fields that are not masked out contain billing information, including credit card numbers, which means the data can still always be linked to a specific person.

3. Does the new Agreement prohibit data mining and profiling?

No. In its Resolution of 11 November 2010, the European Parliament demanded that PNR data "shall in no circumstances be used for data mining or profiling". However, there is no mention of data mining or profiling in the Agreement. It has not been explicitly excluded, as the Parliament has requested, therefore data mining and profiling are still possible and will be done.

4. Does the new Agreement provide sufficient safeguards for European citizens?

No. The proposed Agreement does not provide for sufficient protections and rights for citizens. According to the revised Agreement, any individual is entitled to "request" their PNR data from the DHS. However, since the Agreement does not address what citizens are entitled to receive, the DHS can decline this request. Moreover, the DHS has decided that its use of PNR data is exempt from the Privacy Act even for U.S. Citizens.[3]

---

1 Resolution 5 May 2010 on PNR http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN

2 Article 29 Data Protection Working Party, and to the letter of 6 January 2012 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf

3 As confirmed by a first court decision in Hasbrouck vs. CBP, see http://papersplease.org/wp/2012/01/24/first-rulings-in-our-lawsuit-over-dhs-travel-records

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

It should also be noted that citizens are not informed when their data is being accessed. According to US organisation Friends of Privacy: “Europeans cannot, as the agreement suggests, obtain independent and adequate relief from unlawful actions by the US Executive Branch (USG) by appealing those decisions under the Administrative Procedures Act (the APA).”[4]

5. Is the Agreement proportionate and necessary?

No. The Article 29 Working group points out in its letter dated 6 January 2012 to the LIBE committee that, in order to make “PNR data of all (...) passengers - nearly all of them being innocent and unsuspected citizens - available to foreign law enforcement agencies”, irrefutable proof is required to show that the agreement is necessary and proportionate. So far however, the Commission has failed to prove that the use of PNR data is necessary and proportionate in order to effectively combat terrorism. Instead, the Commission stated that the Agreement was necessary because the USA want access to the data. This misleading claim ignores the test that needs to be carried out on the necessity of data transfer, use and retention for fighting terrorism and serious transnational crime.

The European Parliament has repeatedly called on the Commission “to provide it with factual evidence”[5], but no privacy impact assessment has been carried out, and no systematic evidence apart from a few anecdotes has been provided by the European Commission.

6. Why has the Agreement not taken the form of a treaty?

In its Resolution from 5 May 2010, the European Parliament had asked for the Agreement with the USA to take the form of a Treaty. This has been ignored. Simply because the US has demanded it, the only option available is an Agreement which is not going to be binding on the US and does not require any further US approval. However, it does require ratification by both by Council of the EU (national governments of EU members) and the Parliament. As it is not a Treaty, the Agreement cannot be enforced in US courts. This creates still further legal uncertainty for European citizens.

According to a DHS testimony to Congress, 5 Oct. 2011, an Agreement is crucial “to protect U.S. industry partners from unreasonable lawsuits, as well as to reassure our allies, DHS has entered into these negotiations.”[6] The purpose, therefore, is to legitimise current illegal processing of European data by companies on which US jurisdiction is being imposed.

7. Does the Agreement provide sufficient accountability and oversight?

No. Article 8.3 of the Charter of Fundamental Rights explicitly demands an independent body, as does jurisprudence of the European Court of Justice[7]. However, the oversight structure mentioned in Article 14 of the Agreement does not foresee an independent body – merely an “independent review”.

8. Does the Agreement foresee sufficient protections for onward transfers?

No. In its Resolution of 5 May 2010, the EP asked for sharing PNR data with third countries to be in line with EU data protection laws. The Agreement however does not foresee any compliance with European data protection laws nor does it give more detailed information on how the terms of the Agreement or any other safeguards can practically be implemented. This is exactly the approach criticised by **all** political groups in the debate on data protection in the February 2012 Parliament plenary session.

Therefore, EDRi calls on the MEPs to not give its consent to the conclusion of the Agreement.

4 Steinhardt, Chair of Friends of Privacy http://papersplease.org/wp/wp-content/uploads/2012/01/pnr-agreement-steinhardt-summary.pdf

5 Resolution 11 November 2010 on EU external strategy on PNR http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0397+0+DOC+XML+V0//EN

6 Testimony of David Heyman, Assistant Secretary, Office of Policy, before the House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence https://www.dhs.gov/ynews/testimony/20111005-heyman-info-sharing-privacy-travelers.shtm

7 See: Commission vs. Federal Republic of Germany of 9 March 2010, C-618/07