F.A.Q. EU-US PNR Agreement

March 2012

1) Does the EU-US PNR Agreement meet the European Parliament's conditions for consent?

It does not meet the conditions for consent, adopted by the European Parliament in its two 2010 resolutions.

The **necessity** for mass collection and storage of PNR data must be demonstrated, supported by factual evidence for each of the stated purposes: the European Commission has only insufficiently and partially demonstrated the necessity and proportionality of the mass collection and storage of data. A detailed justification for each of the stated purposes (counter terrorism and fighting serious transnational crime) and for each of the methods of processing (re-actively, real time and pro-actively), as requested by the European Parliament, has yet to be given.

The **proportionality** must be demonstrated: the necessity of ***bulk transfers*** of PNR data has not been demonstrated, the European Commission has insufficiently explored alternative, less intrusive measures, for example the use of API or ESTA data for the identification of suspects.

The **purpose** must be limited clearly and strictly to counter terrorism and the fight against serious transnational crime, on the basis of clear legal definitions based on definitions in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant: Article 4(1) limits the use of PNR tot the fight against terrorism and serious transnational crime, although there is no mention of legal instruments. However, Art 4(2), 4(3) and 4(4) also allow for the systematic use of PNR for other, unspecified purposes, i.e. customs, immigration checks or public health. Therefore there is no limitation of purpose.

Compliance with data protection legislation at national and European level: see FAQ question 5.

The method of transfer must be **"push"** only: in the 2011 Agreement, carries shall be required to use the 'push' system, but DHS retain the option to "pull" data from the European computer systems. The 2004 agreement stipulated a switch to "push", and the 2007 Agreement already imposed a deadline on air carriers to switch to push no later than 1 January 2008, but this obligation has not been enforced by the European Commission. The 2010 Joint Review Report raised "*concerns both as regards the amount of ad hoc requests but also the fact that DHS executes such request by pulling the data*". AEA figures show that there are up to tens of thousands of "ad hoc pulls" each month.

PNR data shall in no circumstances be used for data mining or **profiling**: in the 2011 Agreement, nothing is written on profiling, but is not excluded either. Article 7 reads that "the US shall not make decision (...) based solely on automated processing and use of PNR", but from the EU PNR proposal it is evident that PNR data are run against pre-determined assessment criteria to identify persons previously 'unknown', i.e. profiling.

The **onward transfer** of data by the recipient country to third countries must be in line with EU standards on data protection, to be established by a specific adequacy finding: although some safeguards are contained in the 2011 agreement, including the duty to inform the competent authorities of the Member State concerned and the express understandings that incorporate data privacy protections, the purpose of onward transfers is

not particularly specified and not directly linked even to the very broad purposes mentioned in Article 4. No real progress has been made since the 2004 Agreement.

Results must be immediately shared with the relevant authorities of the EU and of the Member States (**reciprocity**): there is an improvement vis-à-vis the 2007 Agreement on the issue of law enforcement and judicial cooperation. In 2007, law enforcement and judicial cooperation was not yet of a binding nature, and in the 2011 Agreement Article 18 ensures that DHS "*shall provide*" information "*as soon as practicable*". However, information only needs to be shared when it concerns cases under examination or investigation relating to terrorism (Article 4(1)(a)) or to serious transnational crimes (Article 4(1)(b)). The other purposes mentioned in Article 4 fall outside of this obligation to cooperate.

The **legal basis** of the Council Decision concluding the agreement must include Article 16 TFEU: the legal basis does not include Article 16.

Appropriate mechanisms for independent **review**, **judicial oversight** and **democratic control**: Article 13 refers to existing US laws, and Article 21 of the EU US PNR Agreement stipulates that the "*Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public*." As a result, the provisions in the 2011 EU US PNR Agreement do not confer any new rights to EU citizens beyond existing US legislation. The future involvement of US Congress in overseeing the application of the EU US PNR Agreement is a step forward.. However, Article 14 still lacks independent oversight as required under the jurisprudence of the European Court of Justice and the Charter of Fundamental Rights.

Other issues:
retention period: in the 2004 Agreement, data were stored for 3,5 or 8 years and subsequently destroyed. In the 2007 Agreement, data were stored for 15 years and DHS “expects” for PNR to be subsequently deleted. In the 2011 Agreement, data will be stored indefinitely. Data will be retained 10 or 15 years after which the data will be anonymized, but not deleted..

sensitive data: in the 2004 Agreement, the use of sensitive data was not allowed. In 2007, the use of sensitive data was allowed "if necessary, in an exceptional case". The 2011 Agreement states that "access to, as well as the processing and use of sensitive data shall be permitted in exceptional cases".

2) Is this EU-US PNR Agreement better than no Agreement?

If the Agreement is rejected, international law will still apply, including the OECD 1970 guidelines on data protection, to which both EU and US are signatories.

With regards to redress for individuals, the EU-US PNR Agreement does not confer any new rights to EU citizens that they do not already have without this Agreement. The Freedom of Information Act, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and other provisions of US law will also apply without the EU US PNR Agreement. The US have taken an administrative decision for the Privacy Act to apply to non US citizens, however since 2010 the use of PNR data has been exempted from the Privacy Act.

Article 13 of the EU-US PNR Agreement on "Redress for Individuals" reads that "*Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law*."

At first sight, the enhanced level of detail appears to be a clear improvement. However, as Article 13 refers back to US laws, and Article 21 of the EU-US PNR Agreement stipulates that the "*Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public,*" **the Agreement does not confer any new rights to EU citizens**.

The difficulty in case of a rejection of the Agreement is the absence of a legal base for the transfer of PNR data. This is problematic for the carriers.

3) What will happen if the European Parliament gives or withholds consent to the EU-US PNR Agreement?

If the European Parliament gives its consent to the 2011 EU-US PNR Agreement, the procedure on the 2007 Agreement will automatically be considered to have lapsed.

If no consent is given, Parliament will have to vote on the 2007 Agreement, which will continue to apply provisionally until it expires in July 2014. However, as in 2010 Parliament felt unable to give consent to the 2007 Agreement, it is unclear why it would decide to give its consent in 2012 to the very same Agreement. If Parliament also withholds its consent to the 2007 Agreement, the transfer of PNR data by air carriers has no legal base that ensures the transfer of data is in line with EU law.

In case of a rejection of an EU-US agreement, Member States do not automatically have the right to conclude bilateral PNR agreements with the US. And it must be kept in mind that not all Member States have endorsed the EU-US PNR Agreement in Council. On the other hand, most Member States already have bilateral agreements or memoranda of understanding with the US, which include a reference to passenger data. These bilateral agreements, including the transfer of passenger data, are a condition set by the US for visa free travel to the US.

It is unlikely that in the absence of an agreement the data transfer will stop. It is not very likely that the air carriers will risk high fines or withdrawal of their landing rights. In the case of Canada, the Adequacy Decision of the Agreement serving as a legal base for the data transfer lapsed in 2009, but data have been transferred without any difficulty since. In addition, with or without agreement, the US always have access to PNR data by way of broad subpoenas. The data flow will therefore not be affected.

However, without an adequate legal base, the transfer of data by carriers is open to legal challenge, as it violates EU data protection laws.

4) What are the differences between the PNR agreement with Australia and the one with the US?

The purpose of the EU Australia PNR Agreement has been considerably tightened, to include only the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime. Clear definitions of both terms are provided for in the Agreement, on the basis of the relevant EU instruments. Close monitoring of the application of the Agreement will have to demonstrate that the purpose definition is sufficiently precise, and does not leave room for systematic use of PNR for other purposes. The method of transfer of the data is push only. Besides, EU citizens have a right to effective administrative and judicial redress in Australia, and data protection safeguards concerning access, rectification, erasure, are data security are ensured. Sensitive data will not be used.

However, a number of the criteria set by the European Parliament have not been met completely. With regards to the conditions on the 'legal basis', 'profiling', 'necessity' and 'proportionality', the same comments apply as made in FAQ question 2 and therefore the same concerns exist as with the proposed EU US PNR Agreement .

The EU Australia Agreement was adopted on Thursday 27 October 2011.

5) Is the EU US PNR Agreement compatible with the EU Treaties and EU data protection laws?

An international agreement to be concluded by the European Union must, like any other act of secondary law, comply with primary EU law, including the Charter on Fundamental Rights. In the present case, the EU institutions / EU member states are bound by Article 16 TFEU, Article 8 of the Charter of Fundamental Rights, and by Article 8 ECHR. In addition, account must have been taken of Council of Europe Convention 108 and the OECD Guidelines of 1970.

When processing personal data, a number of principles must be taken into account. Generally, the collection of personal data is allowed only for specified, explicit and legitimate purposes and shall be processed lawfully and adequately only for the same purpose for which data were collected. Data must be relevant and not excessive, and they shall be accessible to data subjects, rectified if inaccurate and, where this is possible and necessary, completed or updated. Data shall be, when no longer required for the same purpose for which data were collected, erased or made anonymous. Further processing for another purpose is permitted when compatible with the purposes for which the data were collected, when the competent authorities are authorized to process such data for such other purpose, and when processing is necessary and proportionate to that other purpose. Personal data can be transmitted to third States if the EU Member State from which the data were obtained has given its consent to transfer or the third country ensures an adequate level of protection, subject to derogations. Oversight by independent authorities is required.

Fundamental rights like the right to private life and the right to protection of personal data are not absolute rights but qualified rights; an interference with a person's fundamental rights is acceptable in cases where the interference can be justified. To justify this interference, three conditions must be fulfilled.
1) The interference must be in accordance with the law, as defined by the European Court of Human Rights, stating that *"the law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision…"*
2) The interference must pursue a legitimate aim, being national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, and the protection of the rights and freedoms of others.
3) The interference must be necessary in a democratic society.

In the Agreement, the purposes for the collection of PNR data are not specified and explicit, and ambiguity remains to the effect that the law is not "*accessible and foreseeable…and formulated with sufficient precision*"; the collection of PNR data happens for a different reason than the transfer or processing the data; the necessity and proportionality of the massive and indiscriminate transfer and long term storage of all PNR data has not been demonstrated; the data subject rights seem not to be practically enforceable, so the right of redress is not in line with EU standards; the justification for the retention period is completely missing; and the guarantees for onward transfer are deficient as well as independent judicial supervision.