Brussels, 6 April 2010
D(2010) 5054

Juan Fernando LÓPEZ AGUILAR
Chairman of the Committee on Civil Liberties, Justice and Home Affairs
European Parliament
B-1047 Brussels

Dear Mr. Lopez Aguilar,

Thank you again for your letter of 8 January 2010 asking for the Art. 29 WP's assessment of the PNR agreements the EU signed with Australia and the US.

In my letter of 5 February to you I informed you about the agreement with **Australia** and the fact that we are still waiting for the Commission's answer to our letter of 4 December 2009, where we requested more details concerning the implementation of the agreement.

So far the Commission has not replied and I will keep you informed once their answer has arrived.

Regarding the **US PNR** agreement I promised to come back to you after the joint review carried out in February of this year which included the participation of a representative of the Art. 29 WP.

The joint review proved indeed helpful as all major issues and concerns could be discussed and the review team got direct information from DHS officials to their questions. The members of the team also had the possibility to see how passenger data are processed and used by the competent US authorities. In light of this positive experience the Art. 29 WP expects that future joint reviews will take place more regularly. The first joint review was conducted in 2005 and the one carried out in February was only the second one.

I am confident that the report on the mission to be drafted by the Commission will be forwarded to you soon. The representative of the Art. 29 WP taking part in the joint review was also involved in the drafting of the report.

In your letter you ask specific questions regarding the existing arrangement and I will answer them as follows.

- **Proportionality**

The US PNR agreement foresees the carriers' obligation to transfer PNR data collected by the air carriers for all US bound flights. The data are provided in bulk whether travellers raise any suspicion or not. The vast majority of passengers are innocent people who leave the US after having finished their business plans or vacation. It is legitimate for each country to check the eligibility of travellers coming to that country, and passenger data might be a means of doing so.

The passenger's data, however, are stored for a long time for later use even if the traveller has not committed any offence or crime during his stay and perhaps he will never return to the US. This collection of a great number of passenger data and their retention by a foreign nation constitutes a great intrusion into the privacy of individuals and raises, of course, doubts about the proportionality of such a scheme. In some Member States the storage of data for later analysis without any concrete reason raises even constitutional concerns. For that reason it is of great importance to strike the right balance between fundamental rights of individuals as enshrined in EU legal instruments and national laws on the one hand and the right of another state to know who is crossing its borders on the other hand and to what extent and under which conditions and guarantees the security interests of that requesting state prevail over national applicable law.

- **Elements of context - the broader scheme of personal data collection**

However, to come to a proper assessment of the US PNR agreement it is not enough to analyse the scheme itself but one has also to look at the context in which this arrangement is one albeit important part. You might know that the agreement was only the first step in a whole series of measures aimed at collecting passenger data.

The first agreement covering the transfer of API[1] and PNR data was signed in 2004 following arduous negotiations with the US Government after the US threatened to withdraw the EU air carriers' landing rights if they didn't provide passenger data. The first agreement[2] finally put the existing data transfer on a legal basis and regulated data protection issues which are at the core of the previous and present arrangements.

Since then the US has also introduced "APIS final[3] " requesting air carriers to submit the API data of their passengers prior to departure including their address in the US. Normally the address in the US is not collected by the carriers as it is not necessary for the carriage contract.

Furthermore, since January 2009, the US has made ESTA[4] compulsory demanding the transmission of passenger data in an electronic form prior to departure from citizens of so-called Visa Waiver countries who don't need a visa. ESTA asks for details which include the physical and mental health of a passenger and other sensitive information.

---

1 API (advance passenger information) contained in identity documents such as passports and visas

2 See Art. 29 WP's opinions WP 87 adopted on 29 January 2004 and WP 95 adopted on 22 June 2004

3 APIS Final Rule of 4 October 2005

4 ESTA: Electronic System of Travel Authorization replacing the I-94 paper form. The Art. 29 WP provided the Commission with a preliminary assessment of this scheme in July 2008

Moreover, each passenger is fingerprinted and photographed when arriving in the US.
The US is currently upgrading its technical equipment at airports allowing for the capture of 10 fingerprints of all travellers.

Given these developments it becomes obvious that the US has put in place a border control system which obliges all passengers to provide much more personal information than just API and PNR data if they want to enter the US. The data collected can be and are cross-referenced and matched against watch lists and other relevant information. When putting the PNR scheme in this context it clearly emerges that the data provided by each traveller before boarding a plane render him highly transparent and allow for extensive profiling in particular if passengers travel regularly to the US. It is this perspective that needs to be kept in mind if you want to come to a proper assessment of the proportionality of the PNR system.

- **Retention**

The information additional to PNR data including biometric features (fingerprints and photos) and highly sensitive details contained in the ESTA forms are stored for even longer periods than PNR data[5] which also explains why the US left the door open to an extended retention period for PNR data. Although the agreement's side letter foresees in general a 15-year storage period, the US side expects that "EU PNR data shall be deleted at the end of this period; questions of **whether and when** to destroy PNR data….will be addressed by DHS and the EU as part of future discussions."

The Art. 29 WP considers the retention period as one of the most important issues of any passenger data scheme. In its previously adopted opinions on such programmes it has always objected to extended and general retention periods but has advocated a more nuanced approach based on the real necessity of the data. In any case, the 15-year retention period has been considered too long and we believe that an even longer retention period is completely disproportionate. It has to be mentioned here that Australia stores passenger data only for 5.5 years.

It still remains unclear which retention period applies in case data have been shared with other national and foreign agencies. The agreement largely extends the possibilities of sharing passenger data and remains silent on this point.

The Art. 29 WP maintains that the retention period is only one out of several issues that markedly lowered the data protection level of the 2007 agreement in comparison to the previous PNR agreements of 2004 and 2006. In addition to the fact that the level of data protection was lowered by the agreement itself, the US introduced immediately after the signing of the PNR accord amendments to the Privacy law giving exemptions to DHS from responding to requests for personal information held in the Automated Targeting System (ATS) for reasons of national security, law enforcement, immigration and intelligence activities.

[5] ESTA data and biometric data are stored for a period of 75 years

- **Nature of data collected**

The Art. 29 WP's opinion WP 138 describes in a detailed way the features of the agreement and gives a comprehensive overview of data protection related issues. The Art. 29 WP has always supported the fight against terrorism and serious crime and acknowledges that passenger information and specifically API data can be a valuable tool in identifying perpetrators. API data are contained in official documents and are collected prior to boarding. They can be considered reliable information, while any details provided by the passenger are less certain, may be incorrect, insufficient or even misleading. For that reason, the Art. 29 WP would consider a PNR scheme more privacy compliant if in the first instance only API data were transferred and in cases of hints or suspicion PNR data were supplemented on a case-by-case basis.

In the case of the current US PNR agreement, not only has the number of data elements been increased, but DHS can now get information of third persons others than those travelling, and in exceptional cases it may even get sensitive information as defined in Art. 8 (1) of Directive 95/46/EC and other details contained in a PNR record. The data elements "available frequent flyer information", "general remarks including OSI, SSI and SSR information " and "all historical changes" even if they don't always contain sensitive information can be of great importance for profiling passengers, in particular if they are combined with other passenger details as mentioned before. Whether these data elements are indeed necessary for the purposes of the agreement remains questionable. The Art. 29 WP considers the list of 19 data sets which amount to ca. 35 data elements excessive and calls for a reduction of the data elements. We believe that before any future agreement is concluded an evaluation of these data elements should be conducted. The Canadian example[6] clearly shows that fewer data elements are sufficient for the purposes of fighting terrorism and serious crime. Neither the Australian nor Canadian PNR agreements foresee the use of sensitive data.

There is no information available whether passenger information is used for data mining. But the large amount of data available to US authorities could be a source for data mining.

The Art. 29 WP also believes that the filtering of data should be solely done by the carriers. At the moment DHS filters data. This concerns in particular the filtering of sensitive data. From a data protection point of view it would be much more privacy compliant if the data were filtered before transferring them to the recipient, as there is no efficient control over the filtering methods once data have been transferred**.** Such a filtering would be in line with data protection principles as the air carriers as data controllers are responsible for the processing including the transfer to third parties.

- **Purpose limitation**.

Furthermore, the Art. 29 WP is of the view that the purposes for which data can be processed and shared are too broad. The notions of terrorism related crimes and serious crime are not precisely defined anywhere and might be subject to diverging views. The notion of "transnational nature" needs further explanation as well. Not every perpetrator crossing the border has committed a transnational crime.

Also the reasons for which data can be shared need further explanation. In particular, the notion of public security for which passenger data can be shared with other agencies is very

---

6 Canada requests only 25 data elements and does not ask for general information including OSI, SSI and SSR

far reaching and might be used in cases which can't be considered a serious crime. We are convinced that any follow-up agreement should do better in defining the purposes for transferring PNR data.

- **Legal certainty and rights of persons affected**

Both the agreement and the side letter have been published in the US Federal Register. The side letter says in its part V that administrative, civil and criminal enforcement measures are available under US law for violations of US privacy rules and unauthorised disclosure of US records.

Although DHS as a matter of policy has voluntarily extended the rights of the Privacy Act to non-US citizens not covered by this legal instrument, it remains to be seen whether the Privacy Act will be applied in cases of violations. On the other hand DHS has restricted the rights of passengers requesting access to their data as mentioned before following the signing of the 2007 agreement. To date the Art. 29 WP is not aware of any case where violations of US privacy rules have been challenged in US courts.

You might know that the US has no independent data protection supervisory authority and that the question of judicial redress has repeatedly been addressed by the High Level Contact Group. The question of judicial redress remains an outstanding issue to which a final answer still has to be found. For that reason it continues to be a concern and needs to be tackled in future discussions.

- **Method of transfer**

Our major concern apart from the issues described above regards how passenger data are transferred to DHS. The agreement is clear in that PNR data are to be transferred by the carriers using a push method only, once they fulfil DHS technical requirements. There are no exceptions foreseen and a push solution had to be installed on 1 January 2008 at the latest.

In our letter of 4 December 2009 to Commissioner Barrot we informed him that the US is still pulling data in addition to the carriers' pushes even though the technical requirements are in place as confirmed by the EU carriers and the reservation system Amadeus. The US committed to implement the push system in 2004 and this issue has been raised several times by the Art. 29 WP. There are no plausible reasons why the US continues to pull data along with the data pushed by the carries for ad hoc requests. It has to be stressed that the push system agreed with Canada works smoothly and there have been no complaints from the Canadian authorities or the air carriers. EU citizens had to accept a lowered level of data protection when the current agreement was signed, and it is unacceptable that the US is not respecting one of the most important provisions of the agreement.

In this context the Art. 29 WP again regrets that the agreement does not provide for a dispute mechanism so that the US failure to fully migrate to a push system in case the carriers meet DHS requirements could be addressed. The Australian PNR agreement contains such a provision and any follow-up agreement with the US should foresee such a mechanism as well.

- **Assessment of the agreement**

The agreement was signed for a period of 7 years and will expire in 2014. Whether the agreement is terminated before that date or not, the Art. 29 WP considers it of the utmost importance to evaluate the current agreement and assess its usefulness and necessity prior to

signing any follow-up agreement. Such an evaluation should be carried out in addition to any joint reviews that might take place in the future.

In conclusion it can be said that, from a data protection point of view, the US PNR agreement remains a challenge. The current agreement has considerably lowered the level of protection and even now it is not fully complied with when it comes to the change from pull to push. The other existing PNR agreements with Canada and Australia clearly show, however, that it is possible to reach a higher level of data protection where fundamental rights and security interests are better balanced.

We believe that global standards for the transfer of passenger data are more necessary than ever and the agreement with Australia could provide a good starting point.

We hope that the information provided in this letter is useful to you and thank you for your interest in this matter.

We remain available for any additional details you might require.

Yours sincerely

Jacob Kohnstamm
Chairman