Passenger Name Records Agreements
EU agreements with the US and other third countries

After the first PNR agreements concluded after 9/11 proved controversial and encountered legal difficulties, the Commission is now negotiating long-term PNR agreements with three key third countries: the US, Canada and Australia.

Background

Passenger Name Records (PNR) are sets of data compiled by airlines, including information on the booking, frequent traveller information and accompanying passengers. PNR are distinct from API (Advance Passenger Information), which includes the passenger's passport number, validity dates, citizenship and date of birth. Since the terrorist attacks in the US in 2001, which involved commercial aircraft, counter-terrorism agencies worldwide have been looking to use better intelligence to control terrorists' potential use of aircraft.

However, the effectiveness of PNR collection in stopping terrorism is difficult to assess independently, because the authorities are not generally willing to cite concrete examples of how PNR may have helped them to combat specific threats. This is because the cases in question remain confidential.

Existing PNR agreements

A PNR agreement concluded by the EU (EC) with Canada entered into force in 2006. It covers not only PNR, but also API data. This agreement became invalid in 2009, owing to the expiry of the Adequacy Decision (the Commission decision which sets out that the Canadian authorities ensure "adequate" protection of personal data), thus necessitating the opening of negotiations on a new agreement. In 2008, a similar agreement was concluded between the EU and Australia, currently applied provisionally.

The 2004 EU-US PNR agreement

For the US, the first agreement with the EU was conducted immediately after the September 11 terrorist attacks and entered into force in 2004. Specific provisions were dealt with in an annexed document called the "Undertakings".

The agreement and undertakings stipulated that a "pull" system should be temporarily adopted - meaning US authorities would have access to the reservation systems of the carriers. The justification was that the carriers did not have adequate electronic systems in place to transmit the data upon request from the US Department of Homeland Security (DHS) (i.e. a "push" system). Data not accessed manually must be destroyed after 3.5 years.

Perhaps most controversially, after the conclusion of the agreement, the United States wrote a letter to the Council in which they effectively reinterpreted certain aspects of the Undertakings, on the basis of new US laws.

In 2006, the EP initiated a legal challenge to the agreement. As a result, it was annulled by the Court of Justice of the EU in 2006 on the basis that it had an inappropriate legal base.

2007 EU-US PNR Agreement

This led to the conclusion of a 2007 agreement, which in many respects mirrored the terms of the 2004 agreement. After its conclusion, the US wrote to the Council requesting that all documents pertaining to the negotiations leading up to the agreement be kept "in confidence" for at least ten years.

Because of Parliament's refusal to give its consent to the current agreement, in March 2010 after gaining new powers under the Lisbon Treaty, the Commission has had to renegotiate.

Data protection in EU law

The protection of one's personal data is a fundamental right in the EU. As such it is guaranteed by Article 16 TFEU, as well as Article 8 of the Charter of Fundamental Rights.

Data protection is also regulated in secondary law through the 1995 Data Protection Directive (DPD). This is the standard by which EU air carriers must treat PNR under their control. However, the DPD does not apply to data processing operations concerning public security or state security. Thus, once PNR data...
are transferred from the air carriers to public authorities, the level of data protection is lowered significantly.

The new EU PNR agreements

The US-EU agreement

A 20 May 2011 draft of the PNR agreement currently under negotiation has been leaked to the media. Among its key points it stipulates that PNR data may be retained by US authorities in full form for five years; depersonalised (identifying personal details blacked out) and kept for a further ten years (5 + 10). This is significantly longer than the 3.5 years in the 2004 Agreement.

Another key point is that the draft explicitly excludes the creation of any right or benefit to any private parties. This provision, which was also in the 2004 and 2007 agreements, could be used to deny remedies to a party wrongly imprisoned as a result of PNR data transmitted under this Agreement. Such a case occurred between the US and Canada.

Commission legal opinion

An 18 May 2011 opinion of the Commission's legal service on the new US-EU Agreement was also leaked. The opinion questions the legality of the draft on a number of grounds, most notably:

- Definition of "serious crime", in terms of the US right to use the PNR records, to include any offence carrying a prison sentence of one year or greater;
- Period of retention of data for 15 years (5 + 10) disproportionate to requirements;

Criticism of the US-EU Agreement

Mission creep

Human rights groups within the EU and beyond have also warned of the risks of 'mission creep' in terms of the use of PNR.

Although the data collected was originally intended to be used to protect against a small number of (serious) crimes, critics fear that, over time, the remit of data use could be broadened to include civil offences, control of infectious diseases or even to aid private corporate interests.

Lack of universality of US data protection laws

Critics have also noted that unlike the EU, where data protection is considered a fundamental right, and therefore is not conditional on citizenship, US law only affords data protection rights to its own citizens.

Position of the United States

The US maintains that the retention and evaluation of PNR data is vital for stopping transnational terrorism. They claim that 11 of the 19 hijackers involved in the 2001 attacks could have been stopped using PNR data.

The US also feels that countries should respect each other’s legal traditions, noting that the EU and the US have different backgrounds with regard to protection of civil liberties. For the US, the EU is attempting to unilaterally impose its data protection laws on the US.

While accepting that the protection of individual liberties is a core American value, Michael Chertoff, head of the DHS, nevertheless notes that "life is the liberty on which all others depend". He feels that conventional policy tools are inadequate in dealing with the new threats posed by 21st Century terrorism.

Agreements with Australia and Canada

A new agreement has been initialled with Australia. Data retention periods are significantly shorter, at 5.5 years (3 + 2.5), compared to the draft US agreement, Negotiations continue on a new agreement with Canada.

New EU PNR Directive

Both proponents and sceptics of PNR retention agree that a common EU approach is a necessary prerequisite to effective negotiations with third countries. The lack of coordination has already led to some MS seeking bilateral agreements with third countries, an approach which threatens to undermine the EU’s negotiating position.

A proposal for an EU PNR directive was made in February 2011 (Rapporteur: Timothy Kirkhope (ECR, UK)). Notably, the proposal’s retention period is much shorter (30 days + 5 years) than that of the draft EU-US agreement.

Criticism

The proposal has come under fire from human rights groups on a number of grounds. The EU Agency for Fundamental Rights, on request of the EP, has released an opinion that the case for demonstrating that the PNR law was proportionate to the threats faced has not been properly made.