

# Passenger data caught in holding pattern

The legal status of a controversial EU/US pact – allowing the transfer of airline travellers' personal information – has been temporarily salvaged.

By CATRIONA HATTON and CAMILLA BUCHANAN

**O**n Friday 6 October, the EU and US announced that an interim agreement had been reached on the transfer of passenger data, ending a week long period of uncertainty. Negotiations had failed to result in a new agreement by 30 September, the deadline for the expiry of the previous agreement which was struck down by the European Court of Justice because its legal basis was flawed. The new interim agreement is set to be in place for one year, during which time negotiations will continue on a longer term agreement to allow broader consideration of privacy concerns and growing demands from the US. This case well illustrates the difficulties which may arise when Community law, international law and EU inter-institutional tension clash.

The original agreement, entered into during 2004, facilitated compliance by air carriers with US anti-terrorism legislation as well as EU data privacy rules. On the one hand, American anti-terrorism laws require carriers operating passenger flights to or from the States to make Passenger Name Record (PNR) information available to the US authorities – typically consisting of 34 items of personal data on each transatlantic air traveller (including names, addresses, and telephone and credit card numbers) which are checked for signs of suspected terrorists and

criminals. Air carriers that don't comply face a fine of \$6,000 a passenger or may not be granted permission to land on US territory.

On the other hand, the EU Data Protection Directive – as transposed into member states' laws – imposes strict requirements on the processing of personal data. As a general rule, it cannot be sent outside the EU to a country that does not have an adequate level of data protection. For the purposes of the agreement, the EU decided that the US's level of protection to be applied to the passenger data was 'adequate', based on certain (non legally binding) US undertakings. The European Parliament, however, challenged the agreement before the ECJ claiming it lacked an appropriate legal basis and that fundamental (privacy) rights were infringed.

As, unlike a sovereign state, the EU only enjoys the powers conferred by its member states, it must tie an international agreement to a Treaty provision empowering it to approve such a measure. Previous ECJ case law states: "[t]o proceed on an incorrect legal basis is liable to invalidate the act concluding the agreement and so vitiate the Community's consent to be bound by the agreement it has signed."

On 30 May the ECJ struck down the agreement. The EU Data Protection Directive explicitly states that it only applies to the processing of data for strictly commercial reasons

and not for security and criminal law enforcement purposes. Although passengers' personal data were gathered initially on commercial grounds, the Court found that as the subsequent transfer was for the purposes of public security, it falls outside the scope of the EU data privacy rules. Accordingly, the Court concluded that the directive could not be used as the legal basis for assessing the personal data transfer procedure in this context. As this was sufficient to annul the agreement, the Court did not rule on the substance, ie whether the transfer of personal data from the EU to the US breaches passengers' fundamental (privacy) rights. However, to protect legal certainty and allow time for a new deal to be reached, the Court held that the pact could remain in force until 30 September 2006.

To avoid a legal vacuum, and in view of the deadline, EU officials tried to salvage the agreement's substance by negotiating with the US to sign a one-year interim pact, identical in content to the original but with a different legal basis. The proposed new grounds (article 38 of the Maastricht Treaty) allow for international agreements to be entered into in relation to police and judicial co-operation in criminal matters.

However, negotiations stalled when the US wanted to make content changes to the deal, including allowing customs authorities to share

the data more easily with security agencies. The EU preferred that such adjustments form part of discussions over the new agreement that would run from next year. Yet finally the EU agreed on this point on the condition that the other US agencies requesting the data could also guarantee an adequate standard of data protection. A further key element is the move away from the current system in which US authorities 'pull' the information from air carriers' reservation/departure control systems, located within EU member states' territory, towards a system in which the data are 'pushed' from the airlines' computer systems. This is expected to be implemented before the end of the year.

Negotiations on a new longer term agreement will begin almost immediately. Areas of discussion may include the limit on how long data can be kept, who can access it and making the data protection safeguards incorporated in the US undertakings legally binding.

The interim deal gives certainty to the extent that it provides a legal basis for the transfer of data and avoids the complicated situation of multiple bi-lateral agreements between the US and individual EU states. However, it remains to be seen whether the European Parliament's concerns for the protection of EU citizens' data privacy will be effectively addressed in the longer term. ■