Select Committee on European Scrutiny Seventh Report

---

7 Use of Passenger Name Record for law enforcement purposes

(29109) 14922/07 + ADDs 1-2 COM(07) 654	Draft Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes

Legal base	Articles 29, 30(1)(b) and 34(2)(b) EU; consultation; unanimity
Document originated	6 November 2007
Deposited in Parliament	15 November 2007
Department	Home Office
Basis of consideration	EM of 7 December 2007
Previous Committee Report	None
To be discussed in Council	No date set
Committee's assessment	Legally and politically important
Committee's decision	Not cleared; further information requested

Background

7.1 In the operation of their computerised reservation and ticketing systems, major airlines collect data on their passengers for their commercial purposes. Such data, known as the Passenger Name Record (PNR) consists of all that information which is

necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person. Such information includes such matters as the name, address and telephone number of the passenger, information relating to payment, travel itinerary, seat numbers and baggage information, and the travel status of the passenger (including any 'no show' information i.e. history of not turning up for a flight).

7.2 Such PNR data is to be distinguished from information held on an Advanced Passenger Information System (APIS), which is information derived principally from the machine-readable section of national passports and which allows the country of destination access to information about the identities of passengers before they reach the territory of that country. Such data serves to confirm the identity of the passenger, such as nationality, passport number, given names and date of birth but does not otherwise convey any information about the history of the person. At EU level, Council Directive 2004/82/EC[13] requires Member States to ensure that air carriers bringing passengers to the Community's external borders with third States provide advanced passenger information on the passengers they will convey.

7.3 Following the attacks on New York and Washington DC on 11 September 2001, the United States has passed legislation requiring airlines flying to, from, or over the United States to provide the US Department of Homeland Security with electronic access to information held by airlines on their passengers (i.e. PNR data). Canada has passed similar legislation. Such data can be used[14] to identify passengers who may pose a risk, but who are not yet on any government watch-list. Following concerns expressed by the Commission that these requirements could conflict with the obligations assumed by Member States under the Data Protection Directive (Directive 95/46/EC)[15] agreements have been concluded by the European Community (and subsequently the European Union) with the United States and by the European Community with Canada to regulate the transfer of PNR data to those countries by carriers established within the Member States.[16]

7.4 In its declaration on combating terrorism of 25 March 2004 the European Council invited the Commission to bring forward a proposal for a common EU approach to the use of passenger data for law enforcement purposes. The Hague Programme also invites the Commission to bring forward a proposal on the use of PNR data.

The draft Framework Decision

7.5 The draft Framework Decision prescribes obligations relating to the handling of PNR data to be undertaken by the Member States in relation to air carriers operating flights to or from the territory of one or more of the Member States. The proposal does not apply to flights which are internal to the EU, unless the flight connecting two EU airports is part of an international flight. The obligations imposed by the proposal are expressed to be for the purpose of preventing and combating terrorist offences and organised crime rather than crime in general.

7.6 The detailed provisions of the proposal may be summarised as follows. Article 1 sets out the objective of the proposal which is to provide for the making available by air carriers of PNR data on passengers on international flights to competent authorities for the purpose of preventing and combating terrorist offences and organised crime.

7.7 Article 2 sets out a number of definitions. An "international flight" is defined as any flight originating in a third country and scheduled to enter the territory of at least one EU Member State, or one which departs from an EU Member State with a final destination in a third country. "Passenger Name Record (PNR)" is defined as a record of each passenger's travel requirements which contains "all information necessary to enable reservations to be processed and controlled by the booking and

participating air carriers for each journey booked by or on behalf of any person". PNR data is further defined as the data elements described in the Annex to the Framework Decision in so far as these are collected by the air carriers. The Annex lists 19 classes of data including dates of travel, ticket information, payment information including billing address, itinerary, frequent flyer information, the travel status of the passenger (including confirmations, check-in status, 'no show'[17] or 'go show'[18] status), seat number and baggage information and any collected API information.

7.8 The definitions in Article 2 also distinguish the "push method" (whereby carriers transmit PNR data to the competent authority) from the "pull method" (whereby competent authorities gain access to the carrier's database and extract the required data).

7.9 Chapter II of the proposal (Articles 3 to 10) is concerned with the responsibilities of the Member States for handling PNR data, Chapter III (Articles 11 and 12) with data protection, Chapter IV (Articles 13 to 15) with comitology procedure for adopting common protocols and encryption standards and Chapter V (Articles 16 to 20) with final provisions.

7.10 The key provision set out in Article 3 requires each Member State to designate a "Passenger Information Unit" which will be responsible for collecting PNR data from carriers and their intermediaries. The Unit is obliged immediately to delete any data so collected which is additional to that referred to in the Annex, or which would reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or information concerning the health or sex-life of the person concerned. The Unit is to be responsible for carrying out a risk assessment of passengers in accordance with criteria and guarantees provided for under national law. The Unit is also to transmit the PNR data of any relevant individuals to the competent authorities of that Member State. The Unit and the competent authority may process the data for the purposes of preventing or combating terrorism or organised crime but only in order to identify persons or their associates who may be involved in such offences or to update risk indicators for such persons, or to provide intelligence on travel patterns and other trends relating to such offences, or for the purpose of criminal investigations and prosecutions.

7.11 Article 4 provides for the designation of authorities competent to receive PNR data from Passenger Information Units, but such authorities may only include those responsible for the prevention or combating of terrorist offences and organised crime.

7.12 Article 5 requires Member States to adopt measures to ensure that air carriers provide PNR data to the national Passenger Information Unit of the territory of entry, departure or transit, such data to be provided 24 hours before the scheduled flight departure and immediately after flight closure. Article 5(4) requires those air carriers whose databases are established in a Member State to use the "push method" to transfer PNR data. Where the databases are not established in a Member State, Article 5(5) requires the carrier to use the "push method" or where this is not technically possible, to allow the relevant Passenger Information Unit to use the "pull method" to extract the data.[19] Article 5(6) requires Member States to ensure that air carriers inform their passengers on international flights about the provision of PNR data to the Passenger Information Unit, the purposes for which the data is processed, the period of data retention and the possibility of exchanging and sharing such data.

7.13 Article 6 requires Member States to ensure that air carriers may designate an intermediary to which they may make PNR data available, instead of directly to a Passenger Information Unit, but such intermediaries must provide PNR data to such

Units by the "push method" and are to be obliged to keep their databases and carry out processing within the "territory of the European Union".

7.14 Article 7 provides for the exchange of information between Passenger Information Units only where this is necessary in the prevention and fight against terrorist offences and organised crime. Article 8 provides that PNR data may be provided to law enforcement authorities of a third country where the Member State is satisfied that the data will be used only for the purposes of preventing and fighting terrorist offences and organised crime and that the third country will not transfer the data to any other third country without the express consent of the Member State.

7.15 Article 9 requires Member States to ensure that PNR data provided by carriers to a Passenger Information Unit is held for a period of 5 years. After this 5 year period, the data is to be held for a further 8 years, but the data may only be processed with the approval of the competent authority and only in "exceptional circumstances in response to a specific and actual threat or risk" related to terrorist offences and organise crime. On the expiry of this further 8 year period, the data is to be deleted except where it is being used in an ongoing criminal investigation of a terrorist offence or an organised crime against or involving the data subject.[20]

7.16 The data protection provisions in Articles 11 and 12 require the Member States to apply the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation (still under discussion in the Council) to be applied to the processing of PNR data and for such processing to be exclusively for the purposes of preventing or combating terrorist offences or organised crime. Article 12 requires Member States to ensure that Passenger Information Units, intermediaries and competent authorities adopt necessary security measures with respect to PNR data, both to protect its physical security and to prevent any unauthorised processing.

7.17 Articles 13 to 15 provide for a type of comitology procedure for the adoption by the Commission of common protocols and common encryption standards for the transmission of PNR data. For this purpose, the Commission is to be assisted by a Committee of representatives of the Member States, which will be required to give an opinion on the measures proposed by the Commission. Where the opinion of the Committee (adopted by QMV) is in favour of the proposal, the Commission may adopt the proposal. Where the proposals are not in accordance with the opinion of the Committee (or the Committee gives no opinion), the Commission must submit the proposal to the Council, which may adopt it by QMV. Where the Council has neither adopted the proposal nor indicated its opposition within three months, the Commission may adopt the measure.

The Government's view

7.18 In her Explanatory Memorandum of 7 December 2007 the Parliamentary Under-Secretary of State at the Home Office (Meg Hillier) welcomes the proposal as having "the potential to be an important tool to share data in the fight against criminality targeting our borders". The Minister adds the following comment:

"Our view is that this should be a permissive framework which sets a basis for collection and sharing of PNR and enables our authorities to use this data to maintain the security and integrity of our borders. In particular we need to allow the processing and exchange of PNR data for wider border security and crime-fighting purposes such as immigration and customs purposes. We believe it is vital, and possible, to achieve a result that strikes an appropriate balance between the right to privacy and the right to security and will work with Member States towards ensuring the data protection safeguards included in the proposal are appropriate."

7.19 The Minister goes on to refer to a number of issues raised by the proposal. The first of these is the question of scope where the Minister considers that for the proposal to be limited to preventing or combating terrorist or organised crime "would constrain our ability to process this data for the purposes of combating, for example, individual serious crime" and states that the Government "will need to negotiate a wider scope". The Minister points to "key successes" to date through PNR analysis including the offloading of passengers attempting to smuggle swallowed drugs into the UK, identification of a significant number of facilitators including those using falsified documents and a number of serious crime suspects.

7.20 The Minister also notes that the proposal is limited to the collection of data in relation to flights to and from third countries and states that the UK will seek to ensure that the proposal does not restrict the ability of Member States to collect and process data in relation to other modes of transport, or to collect data on intra-EU journeys.

7.21 On the exchange of information with third countries, the Minister notes that the proposal requires that PNR data may only be provided to law enforcement authorities of third countries for the purpose of preventing and fighting terrorist offences and organised crime, and must not be transferred to another third country without the express consent of the Member State providing the data. The Minister comments that "the UK would wish to retain our current legal powers regarding the exchange of data and therefore will need to ensure that any EU legislation enables this".

7.22 The Minister notes that the proposal restricts carriers to providing PNR data 24 hours in advance of travel, and notes that UK carriers would wish to have the flexibility to provide PNR data more than 24 hours in advance. The Minister wishes to see this flexibility reflected in the proposal.

7.23 On the method of data transfer, the Minister notes that carriers established outside the EU are required to permit a Passenger Information Unit to use the "pull" system to extract data, if they do not have the technology to "push" the data. The Minister explains that the Government prefers the "push" system from a data protection viewpoint and would welcome flexibility for the Member States to determine how they wish data to be transferred.

7.24 The Minister reviews the data protection safeguards contained in the proposal and notes that the UK is "fully supportive" of the inclusion of safeguards and will endeavour to ensure that these are as "robust as possible". However, the Minister also comments as follows:

"The Government does intend to undertake further analysis to ensure that those safeguards presented offer appropriate data protection without unduly undermining operational effectiveness. In particular, the UK would not wish to withhold its right to process sensitive data under the conditions of the Data Protection Act 1998. We therefore seek to ensure compatibility in the negotiations between UK policy and the EU proposal position."

Conclusion

7.25 **This is plainly a significant proposal on a subject which has caused controversy. We agree with the Minister that an appropriate balance needs to be struck between the right to privacy of the individual and the need to ensure safety and security. In this regard, we note with some concern the Minister's apparent intention to broaden the scope of the proposal beyond the prevention of terrorism and organised crime. The limited scope of the proposal appears to us to be a key feature of its acceptability to the Member States, and we ask the Minister for her assessment of the extent to which**

any broadening of scope will be negotiable.

7.26 **We also ask the Minister to explain in more detail her concerns over the transfer of data to third countries and what would be necessary to meet these concerns in the text of the proposal.**

7.27 **We note the Minister's somewhat qualified acceptance of the data protection safeguards contained in the proposal and ask her to give an account, in due course, of the further analysis to which the Minister has referred. On this issue, as on the question of scope and transfer of data to third countries, we would be grateful if the Minister would give an account of any views which the Information Commissioner has provided.**

7.28 **In addition to these general points, we have a number of technical points on which we would be grateful for the Minister's view. The first of these concerns the obligations which are apparently imposed directly on carriers by the proposal. We assume that in all cases the obligations will be imposed by national laws implementing the Framework Decision and that in no case will a carrier be addressed directly by the Framework Decision, but we would be grateful if the Minister would confirm the positions.**

7.29 **Secondly, we ask the Minister if Article 8 contemplates any limit of time for the keeping of data by the third country which has received PNR data.**

7.30 **Finally, we note that a 'comitology' procedure is envisaged whereby it is for the Commission to adopt rules on such sensitive matters as common protocols and common encryption standards. We ask the Minister if it is appropriate for such matters to be dealt with in this way.**

7.31 **We shall hold the document under scrutiny pending the Minister's reply.**

---

13 OJ No L 261, 6.8.04, p.24. Back

14 Notably by the technique of 'data-profiling' i.e. the use of data to match the characteristics of someone or something which is potentially worth investigating. Back

15 OJ No L 281, 23.11.95, p.31. Back

16 The agreements with the United States are the subject of a substantial report by the House of Lords European Union Committee HL Paper 108 of 22 May 2007. Back

17 I.e. instances where a passenger fails to report for a flight. Back

18 I.e. instances where a passenger purchases a ticket immediately before boarding a flight. Back

19 Articles 5(4) and (5) are expressed in terms of obligations directly applicable to air carriers. As Framework Decisions are binding only on Member States, and do not entail direct effect, it would seem that the obligations on carriers msut be imposed by the applicable national law. Back

20 It is not clear if the exception for the investigation of terrorist offences is limited to those against or involving the data subject. Back

Previous Contents Next

Commons Parliament Lords Search Enquiries Index

 Prepared 22 January 2008