

U.S. Department of Homeland Security  
Washington, DC 20528



## Homeland Security

European Commission  
ATTN: Director General Jonathan Faull  
ADDRESS  
Brussels, Belgium]

Presidency of the Council of the EU  
ATTN: Ms. Erma Ertman  
ADDRESS  
Helsinki, Finland]

[Dear Jonathan and Markus:]

This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS). For the purposes of this letter, DHS means the Bureau of Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS such as the Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency. We look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

### Sharing and Disclosure of PNR

The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005 the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

Pursuant to Paragraph 35 of the Undertakings (which states that "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law" and allows DHS to "advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings"), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order described above may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32.

In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of

the U.S. government responsible for preventing or combating of terrorism and related crimes as set forth in Paragraph 3 of the Undertakings.

DHS will therefore facilitate the disclosure (without providing unconditional direct electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiration of the Agreement.

#### Early Access Period for PNR

While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system is considered by the EU to be less intrusive from a data privacy perspective. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by U.S. law. Therefore, it is understood that DHS will utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, taking into account the economic impact upon air carriers.

In determining when the initial push of data is to occur, DHS has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offense enumerated in Paragraph 3. Additionally, while there are instances in which the U.S. government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, DHS will act judiciously and with proportionality.

DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance with the Undertakings and will carry out no later than the end of 2006 the necessary tests for at least one system currently in development if DHS's technical requirements are satisfied by the design to be tested. Without derogating from the Undertakings and in order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself must permit any PNR data in the airline reservation or departure control systems to be pushed to DHS in exceptional circumstances where augmented disclosure is strictly necessary to address a threat to the vital interests of the data subject or other persons.

### Data Retention

Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The Agreement will have expired before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions.

### The Joint Review

Given the extensive joint analysis of the Undertakings conducted in September 2005 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

### Data Elements

The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.

With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

### Vital Interests of the Data Subject or Others

Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital interests" encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay. Such data will be protected in a manner commensurate with its nature and used strictly for the purposes for which it was accessed.

Sincerely yours,

Stewart Baker  
Assistant Secretary for Policy