	2004	2007	2011
Purpose Limitation	DHS will use passenger PNR data for CBP purposes for preventing and combating: 1) Terrorism and related crimes; 2) Other serious crimes, including organized crime, that are transnational in nature; 3) Flight from warrants or custody for crimes described above.	DHS uses PNR strictly for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may also be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceeding, or as otherwise required by law. DHS will advise the EU regarding the passage of any US legislation which materially affects the statements made in this letter.	1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting: a. Terrorist offences and related crimes, including b. Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature. 2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court. 3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examinations 4. Paragraphs 1, 2, and 3 of this Article shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.
Retention Period	* on-line access to PNR data to authorized CBP users for a period of 7 days *** access to the PNR data to a further limited amount of CBP users for a period of three years and 6 months** (3,5 years) *** After 3,5 years, PNR data that has not been manually accessed during that period of time, will be destroyed**. * PNR data that has been manually accessed during the initial 3,5 year period will be transferred by CBP to a deleted record file, where it will remain for a period of **eight (8) years** before it is destroyed	* DHS retains PNR data **in an active analytical database for seven years**, after which time the data will be moved to a **dormant, non-operational status, and retained for eight years** and may be accessed only with approval of a senior DHS official and only in response to an identifiable case, threat, or risk. *** DHS expects that EU PNR shall be deleted at the end of this period**;	1. DHS retains PNR in **an active database for up to five years. After the initial six months of this period, PNR shall be depersonalized and masked** (...). Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorized officials. 3. After this active period, **PNR shall be transferred to a dormant database for a period of up to ten years.** This dormant database shall be subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required

			before access. In this dormant database, PNR shall not be repersonalized except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4, paragraph (1)(b), PNR in this dormant database may only be repersonalized for a period of up to five years. 4. **Following the dormant period, data retained must be rendered fully anonimized by deleting all elements which could serve to identify the passenger to whom the PNR relate without the possibility of repersonalization**. 5. **Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived**. This paragraph is without prejudice to data retention requirements for individual investigation of prosecution files.
Sensitive Data	*** CBP will not use "sensitive" data from the PNR.** * CBP will implement, with the least possible delay, an automated system which filters and deletes certain "sensitive" PNR codes and terms which CBP has identified in consultation with the European Commission. * Until such automated filters can be implemented CBP represents that it does not and will not use "sensitive" PNR data and will undertake to delete "sensitive" data from any discretionary disclosure of PNR under paragraphs 28-34.	*** If necessary, in an exceptional case** where the life of a data subject or of others could be imperilled or seriously impaired, **DHS officials may require and use information in EU PNR other than those listed, including sensitive data**. * In that event, DHS will **maintain a log of access** to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. *** DHS will provide notice normally within 48 hours to the European Commission** (DG JLS) that such data, including sensitive data, has been accessed	1. To the extent that PNR of a passenger as collected included sensitive data (i.e. personal data and information revealing racial or ethic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), **DHS shall employ automated systems to filter and mask out sensitive data from PNR**. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4 of this Article. 2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data which shall be filtered out. 3. **Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperiled or seriously impaired. Such**

			data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager. 4. **Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR** containing such data by DHS. However, **sensitive data may be retained for the time specified in the US law for the purpose of a specific investigation, prosecution or enforcement action**.
Push Pull	CBP will "**pull**" passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to "push" the data to CBP	DHS will **immediately transition to a push system** for the transmission of data by such air carriers no later than 1 January 2008 for all such air carriers that have implemented such a system that complies with DHS's technical requirements. For those air carriers that do not implement such a system, the current systems shall remain in effect until the carriers have implemented a system that complies with DHS's technical requirements. Accordingly, DHS will electronically access the PNR from air carriers' reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for the transmission of such data by the air carriers.	1. For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the "**push**" method, in furtherance of the need for accuracy, timeliness and completeness of PNR 2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS. 3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2 of this Article above, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS. 4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the "push" method not later than 24 months following entry into force of this Agreement. 5. DHS may, **where necessary, on a case-by-case basis**, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, **for technical reasons**, to respond timely to such requests in accordance with DHS standards, ***or*, in exceptional circumstances** in order to respond to a specific, urgent, and serious threat, **DHS may require**

			carriers to otherwise provide such access.
Onward Transfer	CBP in its discretion will only provide PNR data to other government authorities including foreign government authorities, with counter terrorism or law enforcement functions, **on a case-by-case basis**, for purposes of preventing and **combating offenses identified in paragraph 3 herein** (see part on purpose limitation)	DHS shares EU PNR data only **for the purposes named in Article I.** DHS treats EU PNR data as sensitive and confidential in accordance with U.S. laws and, at its discretion, provides PNR data only to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security related cases (including threats, flights, individuals and routes of concern) they are examining or investigating, according to law, and pursuant to written understandings and U.S. law on the exchange of information between U.S. government authorities. Access shall be strictly and carefully limited to the cases described above in proportion to the nature of the case. EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient's intended use(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understandings between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS, as described in the second paragraph of this article.	1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with these terms. 2. ***Apart from emergency circumstances***, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement. 3. **PNR shall be shared only in support of those cases under examination or investigation**. 4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity. 5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-4 of this Article shall be respected.
Judicial Redress	38) In certain exceptional circumstances, CBP may exercise its authority under FOIA to deny or postpone disclosure of all (or, more likely, part) of the PNR record to a first party requester, pursuant to title 5, United States Code, section 552(b) (e.g., if disclosure under FOIA "could reasonably be expected to interfere with enforcement proceedings" or "would disclose techniques and procedures for law enforcement investigations...[which] could	DHS has made a policy decision to **extend administrative Privacy Act protections to PNR data** stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S. law**, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction**	1. **Any individual regardless of nationality**, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement **may seek effective administrative and judicial redress *in accordance with U.S. law***. 2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

	reasonably be expected to risk circumvention of the law"). **Under FOIA, any requester has the authority to administratively and judicially challenge CBP's decision to withhold information** (see 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7-103.9); 40) **Requests for rectification of PNR data contained in CBP's database and complaints by individuals about CBP's handling of their PNR data may be made**, either directly or via the relevant DPA (to the extent specifically authorized by the data subject) to the Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs a Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229; 41) In the event that a complaint cannot be resolved by CBP, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security	**of PNR**. Furthermore, PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U. S. Privacy Act and the U. S. Freedom of Information Act (FOIA). **FOIA permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA.** DHS does not disclose PNR data to the public, except to the data subjects or their agents in accordance with U.S. law. Requests for access to personally identifiable information contained in PNR that was provided by the requestor may be submitted to the FOIA/PA Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5-C, 1300 Pennsylvania Avenue, NW, Washington, DC 20229	3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of: (a) the Freedom of Information Act; (b) the Computer Fraud and Abuse Act; (c) the Electronic Communications Privacy Act; and (d) other applicable provisions of U.S. law. 4. In particular, **DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to inquiries including those related to the use of PNR.** DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns resolve travel-related