II

(Actos cuya publicación no es una condición para su aplicabilidad)

COMISIÓN

DECISIÓN DE LA COMISIÓN

de 14 de mayo de 2004

relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*)

[notificada con el número C(2004) 1914]

(Texto pertinente a efectos del EEE)

(2004/535/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [1], y, en particular, el apartado 6 de su artículo 25,

Considerando lo siguiente:

(1) De conformidad con la Directiva 95/46/CE, los Estados miembros sólo permitirán la transferencia de datos personales a un tercer país si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.

(2) La Comisión puede dictaminar que un tercer país garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en la transferencia o conjunto de transferencias de datos y estudiando con especial atención una serie de elementos relevantes para la transferencia, enumerados en el apartado 2 de su artículo 25.

(4) En el ámbito del transporte aéreo, el registro de nombres de los pasajeros (*Passenger Name Records*, PNR) es un registro de los requisitos de viaje de cada pasajero y miembro de la tripulación. El PNR contiene toda la información necesaria para que sea posible la tramitación y control de reservas por parte de las compañías aéreas de la reserva y de las compañías aéreas participantes respectivamente. El término «compañía aérea de la reserva» significa la compañía aérea con la que el pasajero efectuó su reserva original o con la que se hicieron reservas adicionales después del comienzo del viaje. El término «compañías aéreas participantes» significa cualquier compañía aérea a la que la compañía aérea de la reserva ha solicitado que se reserve un sitio para un pasajero en uno o varios vuelos de esa compañía.

(5) El Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*, CBP) del Departamento de Seguridad Interior (*Department of Homeland Security*, DHS) exige a cada compañía dedicada al transporte aéreo internacional de pasajeros con origen o destino en los Estados Unidos que proporcione a dicho Servicio acceso electrónico al PNR, en la medida en que este se elabora e incluye en el sistema electrónico de reservas de la compañía.

(6) Los requisitos relativos a los datos personales incluidos en los PNR de pasajeros de vuelos que se han de transferir al CBP se basan en una ley promulgada por los los Estados Unidos en noviembre de 2001 [2] y en los reglamentos de aplicación aprobados por el CBP con arreglo a la mencionada ley [3].

[1] DO L 281 de 23.11.1995, p. 31; Directiva modificada por el Reglamento (CE) nº 1882/2003 (DO L 284 de 31.10.2003, p. 1).

[2] Título 49 del *United States Code*, sección 44909(c)(3).

[3] Título 19 del *Code of Federal Regulations*, sección 122.49b.

(7) La legislación estadounidense en cuestión se refiere a la intensificación de la seguridad y de las condiciones en las que se permite la entrada y salida del país de las personas, cuestiones sobre las que los Estados Unidos tienen la facultad soberana de decidir dentro de su competencia. Por otra parte, los requisitos establecidos son coherentes con todos los compromisos internacionales que ha asumido dicho país. Los Estados Unidos son un país democrático, un Estado de Derecho y con una sólida tradición de libertades civiles. La legitimidad de su proceso legislativo y la solidez e independencia de su poder judicial no se cuestionan. La libertad de prensa constituye otra potente garantía frente a cualquier violación de las libertades civiles.

(8) La Comunidad está plenamente comprometida con el respaldo a los Estados Unidos en la lucha contra el terrorismo, dentro de los límites fijados por el Derecho comunitario. El Derecho comunitario permite determinar el equilibrio necesario entre las exigencias de la seguridad y el respeto de la vida privada. Por ejemplo, el artículo 13 de la Directiva 95/46/CE establece que los Estados miembros pueden adoptar medidas legales para limitar el alcance de determinados requisitos de dicha Directiva, en caso necesario por motivos de seguridad del Estado, defensa, seguridad pública y prevención, investigación, detección y represión de infracciones penales.

(9) Las transferencias de datos en cuestión corresponden a responsables específicos del tratamiento de datos, en concreto compañías aéreas que tienen vuelos entre la Comunidad y los Estados Unidos, y a un único destinatario en los Estados Unidos, el CBP.

(10) Todo acuerdo para establecer el marco jurídico de las transferencias a los Estados Unidos destinadas al PNR, en particular a través de esta Decisión, debe ser limitado en el tiempo. Se ha acordado un período de tres años y medio. A lo largo de este período, el entorno puede modificarse de manera significativa, por lo que las dos partes están de acuerdo en que será necesario revisar los acuerdos.

(11) El tratamiento por parte del CBP de los datos personales que contienen los PNR de pasajeros de vuelos que se transfieren a dicho Servicio está regido por las condiciones establecidas en los *Compromisos del Servicio de aduanas y protección de fronteras (CBP) del Departamento de Seguridad Interior*, de 11 de mayo de 2004 (denominados en lo sucesivo, «los Compromisos») así como en la legislación nacional estadounidense en las condiciones que se establecen en dichos Compromisos.

(12) Por lo que respecta a la legislación nacional de los Estados Unidos, la Ley de libertad de información (*Freedom of Information Act*, FOIA) es pertinente en el presente contexto, ya que regula las condiciones en las que el mencionado Servicio puede denegar solicitudes de divulgación y mantener de este modo la confidencialidad de los PNR. La Ley regula la divulgación de un PNR a la persona a la que se refiera tal registro; dicha divulgación está íntimamente relacionada con los derechos de acceso del interesado. Se aplica a los ciudadanos estadounidenses y extranjeros indistintamente.

(13) Por lo que respecta a los Compromisos mencionados, tal como se establece en el punto 44 de éstos, lo dispuesto en los Compromisos se incorporará, o ya se ha incorporado, a leyes, reglamentos, directivas u otros instrumentos políticos en los Estados Unidos, por lo que tendrá efectos jurídicos de distinto grado. Los Compromisos se publicarán íntegramente en el Registro Federal bajo la autoridad del DHS. Se trata de Compromisos políticos serios y muy meditados del DHS cuyo cumplimiento será objeto de control conjunto por parte de los Estados Unidos y la Comunidad. Su incumplimiento podrá ser objeto de recurso, según proceda, por las vías jurídica, administrativa y política y, si se mantiene, dará lugar a la suspensión de los efectos de la presente Decisión.

(14) Las normas que aplica el CBP al tratamiento de los datos de los PNR con arreglo a la legislación de su país, así como los Compromisos citados, respetan los principios básicos necesarios para un nivel adecuado de protección de las personas físicas.

(15) Por lo que se refiere al principio de limitación a una finalidad específica, los datos personales de los pasajeros de vuelos incluidos en los PNR que se transfieren al CBP serán objeto de tratamiento para una finalidad específica y posteriormente se utilizarán o volverán a transmitirse únicamente en caso de que ello sea compatible con la finalidad de la transferencia. En concreto, los datos de los PNR se utilizarán estrictamente para los fines de prevención y lucha contra el terrorismo y delitos conexos, otros delitos graves, incluida la delincuencia organizada, que tengan un carácter transnacional y la fuga en caso de orden de arresto o detención por estos delitos señalados.

(16) En cuanto a la calidad de los datos y el principio de proporcionalidad, que han de considerarse en relación con los motivos importantes de interés público por los que se transfieren datos del PNR, los datos que se faciliten al CBP no podrán ser alterados por dicho Servicio. Se transferirá un máximo de 34 categorías de datos del PNR; las autoridades estadounidenses consultarán a la Comisión antes de añadir nuevos requisitos. La información adicional de carácter personal que se desee obtener como consecuencia directa de datos del PNR se obtendrá de fuentes ajenas a la administración únicamente por vías legales. Por regla general, cada PNR se destruirá al término de un plazo de tres años y seis meses, a excepción de los datos a los que se haya accedido para investigaciones específicas, o en caso de acceso manual.

(17) Por lo que respecta al principio de transparencia, el CBP facilitará información a los viajeros respecto a la finalidad de la transferencia y el tratamiento y a la identidad del responsable del tratamiento en el tercer país, así como información de otro tipo.

(18) En cuanto al principio de seguridad, el CBP toma las medidas de seguridad técnica y organizativa adecuadas a los riesgos que representa el tratamiento.

(19) Se reconocen los derechos de acceso y rectificación, en la medida en que el interesado pueda obtener una copia de los datos del PNR y la rectificación de los datos inexactos. Las excepciones previstas, a grandes rasgos, son comparables con las restricciones que pueden imponer los Estados miembros con arreglo al artículo 13 de la Directiva 95/46/CE.

(20) Las transferencias ulteriores se realizarán, en cada caso específico, a otras autoridades gubernamentales, incluidas las de otros países, con competencias antiterroristas o encargadas de velar por el cumplimiento de la ley, para fines que correspondan a los expuestos en la declaración de limitación a una finalidad específica. También será posible realizar transferencias para la protección de intereses vitales del interesado o de otras personas, en particular en relación con riesgos importantes para la salud, o en el caso de un procedimiento judicial penal, o en otros casos en que la legislación lo exija. Los organismos que reciban los datos están obligados por las condiciones explícitas relativas a la divulgación a utilizar los datos únicamente para los fines mencionados y no pueden transferir posteriormente los datos sin la autorización del CBP. Ningún otro organismo extranjero, federal, estatal o local tiene acceso electrónico directo a datos del PNR a través de las bases de datos del CBP. El CBP denegará la divulgación pública de los PNR con arreglo a las excepciones establecidas por las disposiciones pertinentes de la FOIA.

(21) El CBP no utiliza datos sensibles del tipo de los mencionados en el artículo 8 de la Directiva 95/46/CE y se compromete a instaurar los medios para destruirlos y a no utilizarlos hasta que se instaure un sistema de filtros destinado a excluir tales datos de los PNR transferidos a los Estados Unidos.

(22) Por lo que se refiere a los mecanismos para garantizar el cumplimiento de estos principios por el CBP, se prevé que el personal de dicho Servicio recibirá formación e información, así como el establecimiento de posibles sanciones a los integrantes del mismo. El respeto de la intimidad en general por parte del CBP será objeto del análisis escrupuloso del Director responsable de la protección de la intimidad (*Chief Privacy Officer*) del DHS, que es funcionario del mismo, pero tiene un amplio margen de autonomía organizativa y debe rendir cuentas cada año al Congreso. Las personas cuyos datos del PNR hayan sido transferidos podrán formular reclamaciones al CBP o, si estas no se resuelven, a dicho Director responsable de la protección de la intimidad del DHS, directamente o a través de las autoridades de protección de datos de los Estados miembros. La Oficina de protección de la intimidad del DHS atenderá mediante tramitación acelerada las reclamaciones que le remitan las autoridades de protección de datos de los Estados miembros en nombre de residentes de la Comunidad, en caso de que el residente considere que su reclamación no ha sido resuelta de manera satisfactoria por el CBP o la Oficina de protección de la intimidad del DHS. El CBP, en colaboración con el DHS, y un equipo dirigido por la Comisión realizarán un examen anual conjunto del cumplimiento de los Compromisos.

(23) Aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la facultad de las autoridades competentes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.

(24) El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la Directiva 95/46/CE, ha emitido dictámenes relativos al nivel de protección de los datos de pasajeros que ofrecen las autoridades estadounidenses, los cuales han servido de guía a la Comisión a lo largo de las negociaciones con el DHS. La Comisión ha tomado nota de estos dictámenes al elaborar la presente Decisión [1].

(25) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado en virtud del apartado 1 del artículo 31 de la Directiva 95/46/CE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

A efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que el Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*; en lo sucesivo, «el CBP») ofrece un nivel adecuado de protección de los datos de PNR que se transfieren desde la Comunidad relativos a vuelos con destino u origen en los Estados Unidos, con arreglo a los Compromisos que figuran en el anexo.

Artículo 2

La presente Decisión se refiere a la adecuación de la protección ofrecida por el CBP con arreglo a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE y no afectará a otras condiciones o restricciones que se impongan en aplicación de otras normas de la Directiva relativas al tratamiento de los datos personales en los Estados miembros.

[1] Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los los Estados Unidos, aprobado por el Grupo el 24 de octubre de 2002, disponible en: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_es.pdf
Dictamen 4/2003 «*on the level of protection ensured in the US for the transfer of passengers' data*», aprobado por el Grupo el 13 de junio de 2003, disponible en: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Dictamen 2/2004 «*on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP)*», aprobado por el Grupo el 29 de enero de 2004, disponible en: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

Artículo 3

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las normas nacionales adoptadas de conformidad con preceptos diferentes a los contemplados en el artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia el CBP, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos en que:

a) la autoridad competente de los Estados Unidos compruebe que el CBP ha vulnerado las normas de protección aplicables, o

b) existan grandes probabilidades de que se estén vulnerando las normas de protección expuestas en el anexo, existan razones para creer que el CBP no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión, se considere que la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados, y las autoridades competentes del Estado miembro hayan hecho esfuerzos razonables en estas circunstancias para notificárselo al CBP y proporcionarle la oportunidad de alegar.

2. La suspensión cesará en cuanto esté garantizado el cumplimiento de las normas de protección y ello se haya notificado a las autoridades competentes de los Estados miembros afectados.

Artículo 4

1. Los Estados miembros informarán inmediatamente a la Comisión de la adopción de medidas basadas en el artículo 3.

2. Los Estados miembros y la Comisión se informarán recíprocamente de cualquier cambio en las normas de protección y de aquellos casos en que la actuación de los organismos responsables del cumplimiento por parte del CBP de las normas de protección que figuran en el anexo no garantice dicho cumplimiento.

3. Si la información recogida con arreglo al artículo 3 y a los apartados 1 y 2 del presente artículo demuestra que los principios básicos necesarios para un nivel adecuado de protección de las personas físicas no están siendo respetados, o que los organismos responsables del cumplimiento por parte del CBP de las normas de protección que figuran en el anexo no están ejerciendo su función, se lo notificará al CBP y, si procede, será de aplicación el procedimiento previsto en el apartado 2 del artículo 31 de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión.

Artículo 5

El funcionamiento de la presente Decisión será supervisado y el Comité creado por el artículo 31 de la Directiva 95/46/CE será informado de cualquier hecho pertinente y, en particular, de cualquier prueba que pueda afectar a la resolución del artículo 1 de la presente Decisión, relativa a que la protección de los datos personales incluidos en PNR de pasajeros de vuelos que se transfieren al CBP es adecuada con arreglo a lo dispuesto en el artículo 25 de la Directiva 95/46/CE.

Artículo 6

Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión, a más tardar en un plazo de cuatro meses a partir de la fecha de su notificación.

Artículo 7

La presente Decisión expirará tres años y seis meses después de la fecha de su notificación, salvo que la Decisión sea prorrogada con arreglo al procedimiento expuesto en el apartado 2 del artículo 31 de la Directiva 95/46/CE.

Artículo 8

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 14 de mayo de 2004.

Por la Comisión

Frederik BOLKESTEIN

Miembro de la Comisión

ANEXO

COMPROMISOS DEL DEPARTAMENTO DE SEGURIDAD INTERIOR — SERVICIO DE ADUANAS Y PROTECCIÓN DE FRONTERAS (CBP)

Con objeto de apoyar el proyecto de la Comisión Europea («la Comisión») para ejercer las facultades que le son asignadas en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE («la Directiva») y adoptar una decisión por la que se reconozca que el Servicio de aduanas y protección de fronteras (*Bureau of Customs and Border Protection* — CBP) proporciona una protección adecuada a efectos de la transmisión por parte de las compañías aéreas de los datos del registro de nombres de los pasajeros [1] (*Passenger Name Records* — PNR), que pueden estar sometidos a la jurisdicción de la Directiva, el CBP se compromete a lo siguiente:

Fundamento jurídico del derecho de obtención del PNR

1. Con arreglo a la ley [título 49, *United States Code* (Código de los los Estados Unidos), sección 44909(c)(3)] y sus reglamentos (provisionales) de ejecución [título 19, *Code of Federal Regulations* (Código de disposiciones federales), sección 122.49b], cada compañía aérea que se ocupe de vuelos internacionales de pasajeros con destino o en procedencia de los los Estados Unidos deberá facilitar al CBP (anteriormente denominado servicio americano de aduanas) un acceso electrónico a los datos del PNR en la medida en que se recopilan y se almacenan en los sistemas automatizados de reserva/control de salidas («sistemas de reserva»).

Uso de los datos del PNR por parte del CBP

2. La mayor parte de los elementos informativos que aparecen en los datos del PNR los puede obtener el CBP mediante el examen del billete de avión y demás documentos de viaje de una persona determinada de conformidad con sus atribuciones ordinarias de control de fronteras, pero la posibilidad de recibir estos datos en forma electrónica va a aumentar significativamente la capacidad del CBP para facilitar viajes de pasajeros de buena fe y llevar a cabo eficazmente una evaluación precoz del riesgo de los pasajeros.

3. El CBP utiliza los datos del PNR estrictamente para impedir y luchar: 1) contra el terrorismo y delitos conexos; 2) contra otros delitos graves, incluida la delincuencia organizada, que sean, por naturaleza, transnacionales; y 3) contra la fuga en caso de orden de arresto o detención por los delitos antes señalados. La utilización de la información del PNR a estos efectos permitirá al CBP centrar sus recursos en preocupaciones de alto riesgo, con lo que se facilitan y se protegen los viajes de pasajeros de buena fe.

Requisitos relativos a los datos

4. Los datos que solicita el CBP aparecen en el anexo A. (Dichos datos así identificados se denominan «PNR» a efectos del presente documento.) Si bien el CBP requiere acceso a cada uno de los treinta y cuatro (34) elementos enumerados en el anexo A, este organismo considera que un PNR individual incluirá en contadas ocasiones un conjunto completo de todos los datos identificados. En los casos en que el PNR no incluya un conjunto completo de todos los datos identificados, el CBP no intentará acceder directamente, desde el sistema de reservas de la compañía aérea, a otros datos del PNR que no estén enumerados en el anexo A.

5. Con respecto a los datos identificados como «OSI» y «SSI/SSR» (normalmente mencionados como observaciones generales y campos abiertos), el sistema automatizado del CBP buscará en estos campos cualquier otro dato identificado en el anexo A. El personal del CBP no estará autorizado a examinar manualmente todos los campos OSI y SSI/SSR, a menos que el CBP considere que la persona objeto de un PNR presenta un elevado riesgo en relación con alguno de los objetivos mencionados en el anterior punto 3.

6. Cualquier información personal adicional buscada como resultado directo de los datos del PNR se obtendrá de fuentes exteriores al gobierno, siempre a través de canales legales, incluso, si procede, utilizando las vías de asistencia judicial recíproca, y únicamente por los motivos mencionados en el anterior punto 3. Por ejemplo, si el número de una tarjeta de crédito figura en un PNR, la información relativa a las transacciones relacionadas con esa cuenta podrá obtenerse en el marco de un procedimiento legal, como una citación emitida por un gran jurado, un mandato judicial o cualquier otra forma autorizada legalmente. Además, el acceso a los registros relacionados con las cuentas de correo electrónico recogidas en un PNR estará sujeto a los requisitos legales de los los Estados Unidos en materia de citaciones, mandatos judiciales, mandatos de detención y otros procedimientos legales, en función del tipo de información que se busque.

7. El CBP consultará a la Comisión Europea en relación con los datos del PNR (anexo A), antes de realizar la revisión, si este organismo tiene conocimiento de campos adicionales de PNR que las compañías aéreas puedan añadir a sus sistemas y el CBP considera que van a mejorar significativamente su capacidad para evaluar el riesgo de los pasajeros o si las circunstancias muestran que va a ser necesario un campo de PNR que anteriormente no lo era para cumplir los objetivos limitados a que se hace referencia en el punto 3 de este documento.

[1] A efectos del presente documento, los términos «pasajero» y «pasajeros» incluirán a los miembros de las tripulaciones.

8. El CBP podrá transferir series de PNR a la administración para la seguridad de los transportes (TSA) con objeto de que esta entidad pueda probar su Sistema informatizado de preselección de pasajeros II (CAPPS II). Tales transferencias no se llevarán a cabo hasta que no se haya autorizado previamente la utilización de datos de los PNR de vuelos nacionales de los los Estados Unidos para las pruebas. La TSA o cualquier otra parte directamente implicada en las pruebas no conservará los datos para las pruebas de los PNR transmitidos con arreglo a esta disposición más allá del período necesario para efectuar tales pruebas, ni los transmitirá a terceros [2]. La finalidad del tratamiento estará estrictamente limitada a las pruebas del sistema CAPS II y sus interfaces y, salvo en situaciones de emergencia que exijan la identificación positiva de un terrorista conocido o una persona con relaciones probadas con el terrorismo, carecerá de toda consecuencia operativa. Según la disposición que requiere un método automatizado de filtrado de los datos, recogida en el punto 10, el CBP habrá filtrado y borrado los datos «sensibles» antes de trasmitir cualquier serie de PNR a la TSA en virtud del presente punto.

Tratamiento de datos «sensibles»

9. El CBP se compromete a no utilizar los datos sensibles (por ejemplo: datos personales que especifican el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos, situación médica o de salud u orientación sexual de la persona) a partir del PNR, como se indica más adelante.

10. El CBP aplicará, con la mayor brevedad, un sistema automatizado para filtrar y borrar ciertos códigos y términos «sensibles» de los PNR, identificados en colaboración con la Comisión Europea.

11. Hasta la implantación de estos filtros automatizados, el CBP declara que no utiliza ni utilizará datos «sensibles» de los PNR y se compromete a suprimir tales datos en cualquier divulgación discrecional del PNR, con arreglo a los puntos 28 a 34 [3].

Métodos de acceso a la información del PNR

12. Con respecto a la información del PNR a la que accede (o recibe) el CBP directamente a partir de los sistemas de reserva de las compañías aéreas con objeto de identificar a individuos que pudiera someter a examen en las fronteras, el personal del CBP sólo accederá (o recibirá) y utilizará información del PNR relativa a personas cuyo viaje incluya un vuelo hacia o a partir [4] de los los Estados Unidos.

13. El CBP «extraerá» la información relativa a pasajeros procedente de sistemas de reserva de las compañías aéreas hasta que éstas puedan poner en marcha un sistema de «transmisión» de datos hacia el CBP.

14. El CBP extraerá la información del PNR relacionada con un vuelo concreto no antes de las 72 horas que preceden a la salida de dicho vuelo, y volverá a comprobar los sistemas un máximo de tres (3) veces entre la extracción inicial, la salida del vuelo desde un punto exterior y su llegada a los los Estados Unidos, o entre la extracción inicial y la salida del vuelo desde los los Estados Unidos, según el caso, para identificar todo cambio en la información. En caso de que las compañías aéreas consigan tener la capacidad de «transmitir» información del PNR, el CBP necesitará recibir la información 72 horas antes de la salida del vuelo, siempre que se le comuniquen también todos los cambios de la información del PNR que se produzcan entre ese momento y la hora de llegada a los Estados Unidos o de salida desde este país [5]. En el caso infrecuente de que el CBP obtenga previamente datos que indiquen que cierta(s) persona(s) que presenta(n) un peligro concreto puede(n) estar viajando a bordo de un vuelo destinado a los Estados Unidos o procedente de este país, o que haga escala en su territorio, el CBP podrá extraer (o solicitar que se le transmitan) datos de los PNR con una antelación superior a 72 horas antes de la salida del vuelo, para garantizar la adopción de medidas adecuadas para impedir o luchar contra alguno de los delitos mencionados en el anterior punto 3. En la medida de lo posible, en los casos en que el CBP deba obtener la información del PNR antes de las 72 horas que preceden a la salida del vuelo, el CBP utilizará los medios habituales de aplicación de la ley.

---

[2] A efectos de esta disposición, el CBP no se considera ni una parte directamente implicada en el proceso de prueba CAPPS II, ni una «tercera parte».

[3] Antes de la aplicación de los filtros automáticos por parte del CBP (mencionada en el anterior punto 10), si existen datos «sensibles» en un PNR divulgado de forma no discrecional por el CBP, como recoge el punto 35, este organismo hará todo lo posible para limitar la divulgación de estos datos «sensibles», con arreglo a la legislación estadounidense.

[4] Esto incluirá a las personas que hagan escala en los los Estados Unidos.

[5] En caso de que las compañías aéreas acordaran transmitir la información del PNR a la CBP, el organismo iniciaría negociaciones con las compañías aéreas sobre la posibilidad de transmitir dicha información con intervalos periódicos entre un plazo de 72 horas antes de la salida del vuelo desde un punto exterior y su llegada a los los Estados Unidos, o en el plazo de 72 horas antes de la salida del vuelo desde los los Estados Unidos, según el caso. El CBP desea utilizar un método de transmisión de la información necesaria del PNR que satisfaga las necesidades de los organismos en materia de evaluación eficaz de riesgos, a la vez que minimice las consecuencias económicas para las compañías aéreas.

Almacenamiento de información del PNR

15. Siempre que lo apruebe la administración de archivos y registros nacionales (*National Archives and Records Administration*) (título 44, *United States Code*, 2101 y ss.), el CBP limitará el acceso en línea a la información del PNR a los usuarios autorizados [6] del CBP durante un período de siete (7) días, tras el cual el número de funcionarios autorizados a acceder a la información del PNR se limitará aún más durante un período de tres años y seis meses (3,5) a partir de la fecha en que se accedió a dicha información (o se recibió ésta) desde el sistema de reservas de la compañía aérea. Tras dicho período de tres años y medio, se destruirán los datos de los PNR que no se hayan consultado manualmente durante dicho período. Una vez transcurridos los tres años y medio, el CBP enviará los datos consultados manualmente a un archivo de registros suprimidos [7], donde permanecerán por un período de ocho (8) años y, a continuación, se destruirán. Este calendario, no obstante, no se aplicará a la información del PNR vinculada a un registro de aplicación específico (dicha información permanecería accesible hasta el archivo del registro de aplicación). En cuanto a los PNR a los que tenga acceso (o reciba) directamente el CBP a partir del sistema de reservas de la compañía aérea durante el período de vigencia de los presentes Compromisos, este organismo respetará los principios de conservación de los datos definidos en el presente punto, sin perjuicio de la posible expiración de los presentes Compromisos con arreglo al punto 46.

Seguridad del sistema informático del CBP

16. El personal autorizado del CBP dispone de un acceso al PNR a través de un sistema Intranet cerrado en el CBP, que está completamente codificado y cuya conexión está controlada por el centro de datos de aduanas (*Customs Data Center*). A la información del PNR almacenada en la base de datos del CBP únicamente tiene acceso en modo «sólo lectura» el personal autorizado, lo que significa que el contenido de la información puede ser reformateado sistemáticamente, pero no se puede alterar sustancialmente de ninguna manera una vez obtenida a partir del sistema de reserva de una compañía aérea.

17. Ningún otro organismo extranjero, federal, estatal o local dispone de acceso electrónico directo a la información del PNR mediante las bases de datos del CBP [incluyendo a través del sistema integrado de información aduanera, *Interagency Border Inspection System* (IBIS)].

18. Los detalles sobre el acceso a la información en las bases de datos del CBP [como por ejemplo: quién, dónde, cuándo (fecha y hora) y cualquier revisión de los datos] los registra automáticamente y los supervisa sistemáticamente el servicio de asuntos internos para evitar la utilización no autorizada del sistema.

19. Sólo determinados funcionarios, empleados o contratistas en materia de tecnología de la información del CBP [8] (bajo supervisión de este organismo) que hayan superado con éxito una investigación sobre antecedentes, dispongan de una cuenta activa, protegida mediante una contraseña (*password*) en los sistemas informáticos del CBP y tengan oficialmente un derecho reconocido para examinar la información del PNR, podrán acceder a esta información.

20. Los funcionarios, empleados y contratistas del CBP están obligados a recibir cada dos años una formación sobre seguridad y confidencialidad de datos, y deben superar un examen. La supervisión del CBP y del sistema CAPPS II se utiliza para controlar y garantizar la conformidad con todos los requisitos en materia de confidencialidad y seguridad de datos.

21. El acceso no autorizado por parte del personal del CBP a los sistemas de reserva de las compañías aéreas o a los sistemas informáticos del CBP que almacenan información del PNR es objeto de graves medidas disciplinarias (que pueden llegar al despido) y pueden dar lugar a condenas penales (multas y/o penas de cárcel por un máximo de un año) (título 18, *United States Code*, sección 1030).

22. Las disposiciones políticas y reglamentarias del CBP contemplan asimismo graves medidas disciplinarias (que pueden llegar al despido) contra cualquier empleado del CBP que revele información procedente de los sistemas informáticos del CBP sin autorización oficial (título 19, *Code of Federal Regulations*, sección 103.34).

23. Podrán imponerse condenas penales (entre las que se incluyen multas y/o penas de cárcel por un máximo de un año) contra cualquier funcionario o empleado de los los Estados Unidos que revele la información del PNR obtenida con motivo de su cometido, cuando dicha revelación no esté autorizada por la ley (título 18, *United States Code*, secciones 641, 1030, 1905).

---

[6] Entre los usuarios autorizados del CBP podemos encontrar empleados destinados en unidades analíticas de las oficinas locales, así como empleados destinados en el centro de orientación nacional (*National Targeting Center*). Como se ha indicado anteriormente, las personas encargadas del mantenimiento, desarrollo o supervisión de la base de datos de la CBP tendrán también acceso a dicha información para tales finalidades limitadas.

[7] Aunque el registro PNR no se suprime técnicamente cuando se transfiere al archivo de registros suprimidos, se almacena como información bruta (no localizable inmediatamente y, por lo tanto, no utilizable en las investigaciones «tradicionales» de aplicación de la ley) y sólo puede consultarlo el personal autorizado de la Oficina de asuntos internos del CBP (y en determinados casos la Oficina del Inspector general en relación con las supervisiones) y el personal responsable del mantenimiento de la base de datos de la Oficina de tecnología de la información del CBP, de acuerdo con sus «necesidades de conocimiento».

[8] El acceso por parte de «contratistas» a cualquier información del PNR contenida en los sistemas informáticos del CBP estará limitada a personas que tengan un contrato con este organismo para ayudar al mantenimiento o desarrollo de su sistema informático.

Tratamiento y Protección de la información del PNR por parte del CBP

24. El CBP trata la información del PNR relativa a personas de cualquier nacionalidad o país de residencia como información sensible en materia de aplicación de la ley y confidencial de carácter personal en el caso de los pasajeros, y como información comercial confidencial en el caso de la compañía aérea. Por consiguiente, no divulgaría dichas informaciones al público, excepto si así lo dispone el presente documento o la ley.

25. La divulgación al público de la información del PNR se rige de manera general por la ley sobre libertad de información (*Freedom of Information Act* — FOIA) (título 5, *United States Code*, sección 552) que autoriza el acceso de cualquier persona (con independencia de su nacionalidad o país de residencia) a los registros de un organismo federal de los los Estados Unidos, excepto si dichos registros (o una parte de ellos) están protegidos frente a la divulgación al público por una exención contemplada en la ley sobre libertad de información. Entre dichas exenciones, esta ley autoriza a un organismo a no revelar un registro (o una parte del mismo) si la información tiene el carácter de información comercial confidencial, si la divulgación de la información pudiera constituir una clara intromisión injustificada en la vida privada, o si la información se elabora a efectos de aplicación de las leyes, en la medida en que se pueda pensar razonablemente que dicha divulgación constituye una intromisión injustificada en la vida privada [título 5, *United States Code*, secciones 552(b)(4), (6), (7)(C)].

26. La normativa relativa al CBP (título 19, *Code of Federal Regulations*, sección 103.12), que rige la tramitación de las solicitudes de información (como por ejemplo la información del PNR) en virtud de la ley sobre libertad de información, contempla específicamente que (con determinadas excepciones en caso de solicitudes procedentes de las personas afectadas por la información) los requisitos de la ley sobre libertad de información en materia de divulgación no son aplicables a los registros del CBP relativos a: 1) información comercial confidencial, 2) material que afecte a la vida privada cuya divulgación pudiera constituir una clara intromisión injustificada en la vida privada, y 3) información recogida con fines judiciales, en los casos en que se pueda pensar razonablemente que su divulgación supondría una intromisión injustificada en la vida privada [9].

27. El CBP decidirá, en relación con cualquier tramitación administrativa o judicial derivada de una solicitud de información del PNR obtenida por compañías aéreas, en el marco de la ley sobre libertad de información, que dichos registros no se pueden divulgar de conformidad con dicha ley.

Transmisión de información del PNR a otras administraciones públicas

28. Con excepción de las transmisiones entre el CBP y la TSA efectuadas con arreglo al punto 8 del presente documento, los servicios del Departamento de seguridad interior (DHS) serán considerados «organismos terceros», sometidos a idénticas normas y condiciones que las restantes administraciones públicas ajenas a dicho departamento para compartir la información del PNR.

29. El CBP, dentro de sus competencias, sólo facilitará la información del PNR a otras administraciones públicas, incluidas las administraciones públicas extranjeras, encargadas de luchar contra el terrorismo o de hacer aplicar la ley, caso por caso, con objeto de impedir o luchar contra el terrorismo u otros graves delitos contemplados en el punto 3 del presente documento. (Las administraciones con las que el CBP puede compartir dicha información se denominarán a partir de ahora «autoridades designadas»).

30. El CBP ejercerá juiciosamente su capacidad de transferir información del PNR para los fines indicados. Este organismo determinará en primer lugar si el motivo de divulgación de la información del PNR a otra autoridad designada se ajusta a la finalidad indicada (véase el anterior punto 29). En tal caso, el CBP determinará si la autoridad designada es responsable de investigar o perseguir las violaciones de un estatuto o reglamento relacionado con este fin, o de exigir su cumplimiento o aplicarlo, cuando a alguno de estos organismos le conste que se ha producido una violación o que ésta puede ocurrir. La justificación de la divulgación deberá examinarse a la luz de todas las circunstancias presentes.

31. Para regular la divulgación de datos de los PNR que puedan transmitirse a otras autoridades designadas, el CBP se considera el «propietario» de los datos y dichas autoridades designadas están sujetas, en virtud de las condiciones expresas de divulgación, a las siguientes obligaciones: 1) utilizar los datos PNR únicamente para los fines previstos en los puntos 29 o 34 del presente documento, según proceda; 2) velar por la eliminación sistemática de los datos de los PNR recibidos, respetando los procedimientos de conservación de registros de la autoridad designada; y 3) obtener la autorización expresa del CBP para cualquier divulgación posterior. El Director responsable de la protección de la intimidad (*Chief Privacy Officer*) del DHS podrá investigar e informar sobre el incumplimiento de las condiciones de transmisión y podrá decidir que la autoridad designada deje de tener derecho a recibir transmisiones posteriores de PNR por parte del CBP.

[9] El CBP aplicaría estas exenciones de manera uniforme, con independencia de la nacionalidad o del país de residencia del titular de los datos.

32. Cada divulgación de información del PNR por parte del CBP dependerá de que el organismo receptor trate estos datos como información comercial confidencial y protegida por ley, o como información personal confidencial sobre la persona afectada, como se indica en los puntos 25 y 26, y que debería considerarse exenta de divulgación en virtud de la ley sobre libertad de información (título 5, *United States Code*, sección 552). Además, se advertirá al organismo receptor de que no se permitirá una posterior divulgación de esta información sin la expresa autorización previa del CBP. Este organismo no autorizará ninguna transmisión adicional de información del PNR para fines distintos de los indicados en los puntos 29, 34 o 35.

33. Las personas empleadas por tales autoridades designadas que divulguen, sin la debida autorización, información del PNR, podrán ser sancionadas penalmente (título 18, *United States Code*, secciones 641, 1030, 1905).

34. Ninguna declaración del presente documento impedirá el uso o divulgación de información del PNR a las autoridades administrativas pertinentes, cuando tal divulgación sea necesaria para la protección de los intereses vitales de la persona afectada o de otras personas, en especial en lo tocante a importantes riesgos para la salud. Se aplicarán a las divulgaciones por estos motivos las mismas condiciones de transmisión recogidas en los puntos 31 y 32 del presente documento.

35. Ninguna declaración del presente documento impedirá el uso o divulgación de información del PNR en cualquier causa judicial penal o si existe una obligación jurídica. El CBP avisará a la Comisión Europea en caso de adopción de cualquier legislación estadounidense que afecte sustancialmente a las declaraciones efectuadas en el presente documento.

Comunicación, acceso y posibilidades de reparación para las personas afectadas por el PNR

36. El CBP proporcionará información a los viajeros sobre los requisitos PNR y las cuestiones relacionadas con su utilización (a saber, información general sobre la autoridad responsable de la recogida de datos, finalidad de la recogida, protección de datos, datos compartidos, identidad del funcionario responsable, procedimientos disponibles de reparación e información de contacto para personas que formulan preguntas, preocupaciones, etc., publicaciones en el sitio web del CBP, en los folletos de viajes, etc.).

37. Las solicitudes por parte de la persona afectada (también denominada «solicitante en primera instancia») para recibir una copia de la información del PNR que figura en la base de datos del CBP acerca de su persona se tramitan en el marco de la ley sobre libertad de información. Estas solicitudes podrán enviarse a: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229; por correo; o entregarse personalmente a: Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. Se puede obtener más información sobre los procedimientos de solicitud en el marco de la ley sobre libertad de información en la sección 103.5 del título 19 del *United States Code of Federal Regulations*. En el caso de una solicitud en primera instancia, el hecho de que el CBP considere, por otro lado, que la información del PNR sea información personal y confidencial sobre la persona afectada o información comercial y confidencial de la compañía aérea no será utilizado por este organismo, en el marco de la ley sobre libertad de información, para ocultar información del PNR a la persona afectada.

38. En determinadas circunstancias excepcionales, el CBP podrá ejercer su autoridad en el marco de la ley sobre libertad de información para denegar o aplazar la divulgación total (o, más probablemente, parcial) del registro PNR a un solicitante en primera instancia, de conformidad con el título 5, *United States Code*, sección 552(b) (por ejemplo, si la divulgación en el marco de la ley sobre libertad de información pudiera previsiblemente alterar las modalidades de aplicación o revelara técnicas y procedimientos de las investigaciones judiciales que, previsiblemente, pudiera provocar un incumplimiento de la misma). En virtud de la ley sobre libertad de información, cualquier solicitante tiene la capacidad de impugnar administrativa o jurídicamente la decisión de un organismo de retener información (título 5, *United States Code*, secciones 552(a)(4)(B); título 19, *Code of Federal Regulations*, secciones 103.7-103.9).

39. El CBP rectificará [10] datos a petición de los pasajeros y de los miembros de la tripulación, de las compañías aéreas o de las autoridades de protección de datos de los Estados miembros de la Unión Europea (en la medida específicamente autorizada por la persona afectada) cuando aquel organismo determine que estos datos figuran en su base de datos y que se justifica una corrección por estar adecuadamente sustentada. El CBP informará a cualquier autoridad designada que haya recibido esa información del PNR sobre cualquier rectificación importante de tales datos.

[10] Al «rectificar», el CBP desea dejar claro que no estará autorizado a revisar los datos del registro PNR de las compañías aéreas a los que tenga acceso. Se tratará, más bien, de crear un registro separado y vinculado al PNR para anotar que se ha determinado la inexactitud de los datos y que se han corregido adecuadamente. Concretamente, el organismo anotará el registro de examen secundario del pasajero para reflejar que determinados datos del PNR pueden ser o son inexactos.

40. Las solicitudes de rectificación de datos de los PNR que figuran en la base de datos del CBP y las denuncias individuales presentadas por los titulares de estos datos en cuanto al tratamiento de los mismos por parte de este organismo deberán enviarse, bien directamente, o bien por medio de las autoridades de protección de datos (en la medida específicamente autorizada por la persona afectada) a la siguiente dirección: Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

41. En caso de que el CBP no pueda resolver la reclamación, ésta podrá remitirse, por escrito, al Director responsable de la protección de la intimidad (Department of Homeland Security, Washington, D.C. 20528), quien examinará la situación y procurará solucionarla ([11]).

42. Además, la Oficina de protección de la intimidad del DHS examinará con urgencia las denuncias que le remitan las autoridades de protección de datos de los Estados miembros de la Unión Europea en nombre de un residente de la Unión Europea, en la medida en que este residente haya facultado a las autoridades a actuar en su nombre y considere que el CBP o el propio Director responsable de la protección de la intimidad del DHS no han tratado adecuadamente su denuncia en materia de protección de datos de los PNR (de conformidad con los puntos 37 a 41 del presente documento). Dicho Director comunicará sus conclusiones y advertirá a las autoridades de protección de datos en cuanto a la adopción de medidas, si se hubiera producido. El Director incluirá en su informe al Congreso una serie de cuestiones sobre el número, el contenido y la resolución de denuncias relativas al manejo de datos personales, tales como el PNR ([12]).

Sobre el cumplimiento

43. El CBP, junto con el DHS, se compromete a celebrar una vez al año o con más frecuencia, si las partes así lo decidieran, un examen conjunto con la Comisión Europea, asistida, si fuera conveniente, por representantes de las autoridades europeas encargadas de garantizar el cumplimiento de la legislación y/o de las autoridades de los Estados miembros de la Unión Europea ([13]), sobre la aplicación de los presentes Compromisos, para contribuir conjuntamente al buen funcionamiento de los procesos descritos en el presente documento.

44. El CBP adoptará reglamentos, directrices u otros documentos políticos que incorporen las declaraciones aquí formuladas, para que los funcionarios, empleados y contratistas de este organismo puedan cumplir los presentes Compromisos. Como se indica en el presente documento, a los funcionarios, empleados o contratistas del CBP que incurran en un incumplimiento de las decisiones de sus organismos, aquí expuestas, se les podrán aplicar medidas disciplinarias graves o sanciones penales, según proceda.

Reciprocidad

45. En caso de que la Unión Europea aplique un sistema de identificación de viajeros de líneas aéreas que exija a las compañías aéreas proporcionar a las autoridades el acceso a la información del PNR de personas cuyo itinerario de viaje en curso incluya un viaje con destino a la Unión Europea o procedente de ésta, el CBP, sobre una base de estricta reciprocidad, instará a las compañías aéreas radicadas en los Estados Unidos a que cooperen.

Examen y expiración de los Compromisos

46. Los presentes Compromisos se aplicarán durante un período de tres años y seis meses (3,5 años) a partir de la entrada en vigor del acuerdo entre los los Estados Unidos y la Comunidad Europea por el que se autorice el tratamiento de datos de los PNR por las compañías aéreas y su transmisión al CBP, de conformidad con la Directiva. Una vez transcurridos dos años y seis meses (2,5 años) de vigencia de los presentes Compromisos, el CBP, junto con el DHS, iniciará conversaciones con la Comisión con el objeto de prorrogar los presentes Compromisos y toda disposición conexa, en condiciones aceptables para ambas partes. Si no fuera posible celebrar un acuerdo aceptable para ambas partes antes de que expiren los presentes Compromisos, éstos perderán su vigencia.

([11]) El Director responsable de la protección de la intimidad del DHS no depende de ninguna dirección dentro del *Department of Homeland Security*. Está obligado por norma a garantizar que el uso de la información personal cumpla la normativa pertinente (véase la nota a pie de página 13). Las decisiones del Director responsable de la protección de la intimidad serán vinculantes para el Departamento y no podrán revocarse por motivos políticos.

([12]) De conformidad con la artículo 222 de la *Homeland Security Act* (Ley de seguridad territorial) de 2002 (Ley pública 107-296 de 25 de noviembre de 2002), el Director responsable de la protección de la intimidad del DHS es responsable de realizar una evaluación del impacto en la vida privada de las normas propuestas del Departamento sobre la vida privada de la información personal, incluido el tipo de información personal recogida y el número de personas afectadas, y debe informar anualmente al Congreso sobre las actividades del Departamento que afectan a la vida privada. El apartado 5 del artículo 222 de la Ley exige a dicho Director que reciba e informe al Congreso sobre todas las denuncias de violaciones de la privacidad.

([13]) Las partes se comunicarán entre sí la composición de los respectivos equipos y podrán incluir autoridades competentes en materia de privacidad/protección de datos, control aduanero y otras formas de aplicación de la ley, seguridad de las fronteras y/o seguridad de la aviación. Las autoridades competentes estarán obligadas a obtener todas las autorizaciones necesarias y asumirán la confidencialidad de las conversaciones y de los documentos a los que pudieran tener acceso. No obstante, la confidencialidad no impedirá que ambas partes presenten un informe adecuado sobre los resultados del examen conjunto a las respectivas autoridades competentes, incluidos el Congreso americano y el Parlamento Europeo. Sin embargo, las autoridades participantes no podrán, bajo ninguna circunstancia, revelar ningún dato personal sobre un determinado individuo, ni ninguna información que no sea pública procedente de los documentos a los que tengan acceso, o cualquier información operativa o propia de la agencia que pudieran obtener durante el examen conjunto. Las partes determinarán conjuntamente las modalidades pormenorizadas del examen conjunto.

No creación de Derecho privado o de precedentes

47. Los presentes Compromisos no crean ni confieren ningún derecho o beneficio a ninguna persona o parte, privada o pública.

48. Las disposiciones de los presentes Compromisos no constituyen un precedente para cualquier negociación posterior con la Comisión Europea, la Unión Europea, cualquier entidad conexa o cualquier Estado tercero en materia de transmisión de cualquier tipo de datos.

11 de mayo de 2004

ANEXO «A»

Datos de los PNR solicitados por el CBP a las compañías aéreas

1. Código de identificación del registro PNR
2. Fecha de reserva
3. Fecha(s) prevista(s) del viaje
4. Nombre
5. Otros nombres en el PNR
6. Dirección
7. Información sobre modalidades de pago
8. Dirección de facturación
9. Teléfonos de contacto
10. Itinerario completo del viaje para el PNR específico
11. Información sobre viajeros frecuentes (referida únicamente a millas recorridas y dirección o direcciones)
12. Agencia de viajes
13. Agente de viajes
14. Información del PNR sobre códigos compartidos
15. Situación de viaje (*travel status*) del pasajero
16. Información sobre PNR escindido/dividido
17. Dirección electrónica
18. Información sobre la emisión de billetes
19. Observaciones generales
20 Número del billete
21. Número de asiento
22. Fecha de emisión del billete
23. Pasajero del que no se dispone de información
24. Números de etiquetado de maletas
25. Pasajero de último momento sin reserva (*Go show information*)
26. Información OSI
27. Información SSI
28. Información sobre la fuente
29. Historial de los cambios aportados al PNR
30. Número de viajeros en el PNR
31. Información sobre el asiento
32. Billetes de ida sólo
33. Toda la información del sistema de información avanzada sobre pasajeros (*Advanced Passenger Information System*, APIS) recogida
34. Información sobre ATFQ (*Automatic Ticket Fare Quote*).