II

(Actos cuja publicação não é uma condição da sua aplicabilidade)

COMISSÃO

DECISÃO DA COMISSÃO

de 14 de Maio de 2004

sobre o nível de protecção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o *Bureau of Customs and Border Protection* dos Estados Unidos

[notificada com o número C(2004) 1914]

(Texto relevante para efeitos do EEE)

(2004/535/CE)

A COMISSÃO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Europeia,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [1], e, nomeadamente, o n.º 6 do seu artigo 25.º,

Considerando o seguinte:

(1) Nos termos da Directiva 95/46/CE, os Estados-Membros devem garantir que a transferência de dados pessoais para um país terceiro só pode realizar-se se o país terceiro em questão assegurar um nível de protecção adequado e a legislação dos Estados-Membros de execução da directiva tiver sido observada antes de efectuada a transferência.

(2) A Comissão pode considerar que um país terceiro garante um nível de protecção adequado. Nesse caso, podem ser transferidos dados pessoais a partir dos Estados-Membros sem serem necessárias garantias adicionais.

(3) Nos termos da Directiva 95/46/CE, a adequação do nível de protecção de dados será apreciada em função de todas as circunstâncias que envolvem a transferência ou o conjunto de transferências de dados, tendo em especial consideração determinados elementos pertinentes relativamente à transferência, enumerados no n.º 2 do artigo 25.º dessa directiva.

(4) No quadro dos transportes aéreos, o «Passenger Name Record» (PNR) é um registo dos dados relativos à viagem de cada passageiro, que contém todas as informações necessárias ao tratamento e controlo das reservas pelas companhias aéreas da reserva e participantes. Para efeitos da presente decisão, os termos «passageiro» e «passageiros» incluem igualmente os membros da tripulação. O termo «companhia aérea da reserva» significa a companhia com a qual o passageiro fez a sua reserva original ou com a qual foram feitas reservas adicionais depois do começo da viagem. O termo «companhias aéreas participantes» significa qualquer companhia aérea à qual a companhia aérea da reserva solicitou um lugar em um ou mais voos para um passageiro.

(5) O *Bureau of Customs and Border Protection* (CBP) do *Department of Homeland Security* (DHS, Ministério da Segurança Interna) dos Estados Unidos exige a todas as companhias aéreas que efectuem voos internacionais de passageiros com destino a ou provenientes dos Estados Unidos que lhe forneçam acesso electrónico aos PNR que estejam compilados e armazenados nos respectivos sistemas automatizados de reservas.

(6) As regras de transferência dos dados pessoais contidos nos PNR de passageiros aéreos para o CBP baseiam-se num diploma aprovado pelos Estados Unidos em Novembro de 2001 [2] e nos regulamentos de execução adoptados pelo CBP ao abrigo desse diploma [3].

[1] JO L 281 de 23.11.1995, p. 31. Directiva com a última redacção que lhe foi dada pelo Regulamento (CE) n.º 1882/2003 (JO L 284 de 31.10.2003, p. 1).

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

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

(7) A legislação norte-americana em questão diz respeito à melhoria da segurança e das condições em que é possível entrar e sair do país, matérias nas quais os Estados Unidos têm poder soberano no âmbito da sua jurisdição. Por outro lado, as regras estabelecidas não são incompatíveis com quaisquer acordos internacionais subscritos pelos Estados Unidos. Os Estados Unidos são um país democrático que respeita os princípios do Estado de Direito e com uma tradição arreigada de liberdades civis. A legitimidade do seu processo legislativo e a força e a independência do seu sistema judicial não estão em causa. A liberdade de imprensa é uma garantia suplementar contra o abuso das liberdades civis.

(8) A Comunidade Europeia está plenamente empenhada em apoiar a luta dos Estados Unidos contra o terrorismo, dentro dos limites impostos pelo direito comunitário. O direito comunitário permite estabelecer o equilíbrio necessário entre as exigências de segurança e o respeito da vida privada. Nomeadamente, o artigo 13.º da Directiva 95/46/CE prevê que os Estados Membros possam tomar medidas legislativas destinadas a restringir o alcance de certas normas da referida directiva, sempre que tal restrição constitua uma medida necessária à protecção da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação, detecção e repressão de infracções penais.

(9) As transferências de dados em questão envolvem responsáveis específicos pelo tratamento desses dados, nomeadamente companhias aéreas que efectuam voos entre a Comunidade Europeia e os Estados Unidos e apenas um destinatário nos EUA, designadamente o CBP.

(10) Qualquer acordo no sentido de criar um quadro legal para as transferências de PNR para os EUA, em particular através desta decisão, deve ser limitado no tempo. Ficou acordado um período de três anos e seis meses. Durante esse período, o contexto pode alterar-se significativamente, pelo que a Comunidade e os Estados Unidos concordam que será necessária uma revisão do acordo.

(11) O tratamento, pelo CBP, de dados pessoais contidos nos PNR de passageiros aéreos transferidos para esta entidade é regido pelos termos da declaração de compromisso do *Bureau of Customs and Border Protection* (CBP) do *Department of Homeland Security* de 11 de Maio de 2004 (doravante «a declaração de compromisso») e na legislação nacional norte-americana, tal como indicado na declaração.

(12) Quanto à legislação nacional dos EUA, a lei relativa à liberdade de informação (*Freedom of Information Act*, ou FOIA) é determinante no presente contexto, na medida em que rege as condições em que o CBP pode recusar pedidos de divulgação e, consequentemente, manter os PNR confidenciais, e rege também a divulgação de PNR à pessoa a quem este diz respeito (titular dos dados), em estreita ligação com o direito de acesso aos dados desse titular. A lei FOIA aplica se sem distinção aos cidadãos dos Estados Unidos e a outros.

(13) Quanto à declaração de compromisso, e tal como previsto especificamente no seu n.º 44, o disposto na declaração será — ou já foi — incorporado em leis, regulamentos, directivas ou outros instrumentos de política dos Estados Unidos, adquirindo assim, em graus variáveis, força de lei. A declaração de compromisso será publicada na íntegra no *Federal Register* sob a autoridade do DHS. Como tal, esta declaração representa um compromisso político sério e ponderado por parte do DHS e o seu cumprimento será objecto de uma revisão conjunta pelos EUA e pela Comunidade Europeia. O não cumprimento pode ser adequadamente combatido pela vias legais, administrativas e políticas e, se for continuado, poderá dar azo à suspensão dos efeitos da presente decisão.

(14) As normas pelas quais o CBP se rege para tratar os dados dos PNR dos passageiros com base na legislação-norte americana e na declaração de compromisso abrangem os princípios básicos necessários a um nível adequado de protecção das pessoas singulares.

(15) Quanto ao princípio da limitação do objectivo, o CBP tratará os dados pessoais contidos nos PNR de passageiros aéreos transmitidos ao CBP com um objectivo específico e, consequentemente, utilizá-los-á ou comunicá-los á-a terceiros apenas se tal não foi incompatível com o objectivo da transmissão. Em especial, os dados dos PNR serão utilizados estritamente para impedir e combater o terrorismo e crimes conexos; outros crimes graves, incluindo o crime organizado, que são, por natureza, transnacionais; e a fuga a mandados judiciais ou à detenção pelos crimes atrás descritos.

(16) Quanto à qualidade dos dados e ao princípio da proporcionalidade, que tem de ser considerado em relação com os importantes motivos de interesse público pelos quais os dados dos PNR são transmitidos, os dados fornecidos ao CBP não serão posteriormente alterados por este organismo. Será transferido um máximo de 34 categorias de dados do PNR, e as autoridades dos Estados Unidos consultarão a Comissão antes de introduzir novas regras. Quaisquer informações pessoais adicionais pedidas como resultado directo dos dados dos PNR serão obtidas de fontes não estatais e apenas pelas vias legais. Regra geral, o PNR será apagado após um período máximo de três anos e seis meses, com excepção dos dados consultados para efeitos de investigações específicas ou manualmente.

(17) Quanto ao princípio da transparência, o CBP fornecerá informação aos passageiros quanto ao objectivo da transferência e do tratamento, bem como à identidade do controlador dos dados no país terceiro, além de outras informações.

(18) Quanto ao princípio da segurança, o CBP tomará as medidas de segurança de carácter técnico e organizacional adequada aos riscos que o tratamento dos dados representa.

(19) Os direitos de acesso e rectificação são reconhecidos, na medida em que o titular dos dados pode requerer uma cópia do PNR e a rectificação dos dados inexactos. As excepções previstas são largamente comparáveis com as restrições que podem ser impostas pelos Estados-Membros ao abrigo do artigo 13.º da directiva 95/46/CE.

(20) As transferências subsequentes para outras autoridades estatais — incluindo estrangeiras — com funções de combate ao terrorismo ou de aplicação da lei serão efectuadas, caso a caso, para fins que correspondam aos definidos na declaração relativa à limitação do objectivo. As transferências podem ainda efectuar-se para a protecção do interesse vital do titular dos dados ou de outras pessoas, designadamente no que diz respeito aos riscos importantes para a saúde, ou no âmbito de qualquer procedimento criminal ou de qualquer outra forma exigida pela lei. Os organismos que recebam os dados estão obrigados, em virtude das condições expressas de divulgação, a utilizar os dados unicamente para os fins previstos, não podendo transferi-los subsequentemente sem o acordo do CBP. Nenhum outro organismo estrangeiro, federal, estatal ou local dispõe de acesso electrónico directo aos dados dos PNR através das bases de dados do CBP. Este recusará a divulgação ao público de dados dos PNR, com base nas excepções previstas nas disposições pertinentes da lei FOIA.

(21) O CBP não utiliza dados sensíveis referidos no artigo 8.º da Directiva 95/46/CE e, até que seja concretizado um sistema de filtros destinado a excluir esses dados dos PNR transferidos para os EUA, compromete-se a introduzir os meios necessários para os apagar e, entretanto, a não os utilizar.

(22) Quanto aos mecanismos de aplicação da lei destinados a garantir o cumprimento, pelo CBP, destes princípios, estão previstas acções de formação e informação do pessoal deste organismo, bem como sanções a aplicar aos seus membros individuais. O respeito pela privacidade em geral por parte do CBP será fiscalizado pelo *Chief Privacy Officer* do DHS, que é um funcionário deste ministério mas tem bastante autonomia e é obrigado a apresentar relatórios anuais ao Congresso. As pessoas cujos dados do PNR tenham sido transferidos podem remeter as suas queixas para o CBP, ou, se estas não tiverem sido resolvidas, para o *Chief Privacy Officer* do DHS, directamente ou através das autoridades responsáveis pela protecção dos dados (APD) dos Estados-Membros. O *Privacy Office* do DHS examinará com urgência as queixas que lhe tenham sido apresentadas pelas APD dos Estados-Membros em nome de residentes da Comunidade, nos casos em que se o residente considere que a sua queixa não foi satisfatoriamente resolvida pelo CBP ou pelo *Privacy Office* do DHS. O cumprimento da declaração de compromisso será objecto de uma revisão conjunta anual, efectuada pelo CBP, conjuntamente com o DHS, e por uma equipa liderada pela Comissão.

(23) No interesse da transparência e a fim de salvaguardar a capacidade de as autoridades competentes dos Estados-Membros assegurarem a protecção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, é necessário especificar as circunstâncias excepcionais em que a suspensão de transferências concretas de dados se pode justificar, mesmo que se verifique um nível de protecção adequado.

(24) O grupo de trabalho «Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais», criado pelo artigo 29.º da Directiva 95/46/CE, emitiu pareceres sobre o nível de protecção previsto pelas autoridades dos Estados Unidos para os dados dos passageiros, os quais guiaram a Comissão ao longo da negociação com o DHS. A Comissão tomou em consideração estes pareceres na preparação da presente decisão [1].

(25) As medidas previstas na presente decisão são conformes com o parecer do comité criado pelo n.º 1 do artigo 31.º da Directiva 95/46/CE,

ADOPTOU A PRESENTE DECISÃO:

Artigo 1.º

Para efeitos do n.º 2 do artigo 25.º da Directiva 95/46/CE, considera se que o *Bureau of Customs and Border Protection* (CBP) dos Estados Unidos assegura um nível adequado de protecção dos dados dos PNR transferidos a partir da Comunidade no que diz respeito a voos com destino a ou provenientes dos Estados Unidos, em conformidade com a declaração de compromisso que figura no anexo I.

Artigo 2.º

A presente decisão diz respeito ao nível adequado de protecção assegurado pelo CBP, a fim de dar cumprimento ao disposto no n.º 1 do artigo 25.º da Directiva 95/46/CE, e não afecta outras condições ou restrições à aplicação de outras disposições da referida directiva relativas ao tratamento de dados pessoais nos Estados Membros.

[1] Parecer 6/2002 sobre a transmissão para os Estados Unidos de informações sobre o manifesto de passageiros e outros dados provenientes das companhias aéreas, adoptado pelo grupo de trabalho em 24 de Outubro de 2002, disponível em: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf
Parecer 4/2003 sobre o nível de protecção garantido nos Estados Unidos para a transferência de dados dos passageiros, adoptado pelo grupo de trabalho em 13 de Junho de 2003, disponível em: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Parecer 2/2004 sobre a protecção adequada dos dados pessoais contidos nos PNR de passageiros aéreos transferidos para o *Bureau of Customs and Border Protection* (CBP) dos Estados Unidos, adoptado pelo grupo de trabalho em 29 de Janeiro de 2004, disponível em: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

Artigo 3.º

1. Sem prejuízo dos poderes das autoridades competentes dos Estados-Membros no que se refere à adopção de medidas para garantir o respeito das disposições nacionais adoptadas por força de outras disposições para além das previstas no artigo 25.º da Directiva 95/46/CE, as referidas autoridades podem exercer os poderes de que dispõem para suspender a transferência de dados para o CBP, a fim de proteger as pessoas no que respeita ao tratamento dos seus dados pessoais, sempre que:

a) A autoridade norte-americana competente verificar que o CBP desrespeita as normas de protecção aplicáveis; ou

b) Seja altamente provável que as normas de protecção constantes do anexo I não estão a ser cumpridas, existam motivos suficientes para crer que o CBP não toma ou não tomará as decisões adequadas na altura devida para resolver o caso em questão, a continuação da transferência dos dados implique o risco iminente de causar graves prejuízos às pessoas em causa e as autoridades competentes dos Estados-Membros tenham envidado esforços razoáveis, dadas as circunstâncias, para facultar ao CBP informação e oportunidade para responder.

2. A suspensão cessará assim que o respeito das normas de protecção estiver assegurado e a autoridade competente do Estado-Membro em questão seja disso informada.

Artigo 4.º

1. Os Estados-Membros devem informar imediatamente a Comissão da adopção de medidas ao abrigo do artigo 3.º

2. Os Estados-Membros e a Comissão devem ainda manter-se mutuamente informados de qualquer alteração nas normas de protecção e dos casos em que os organismos responsáveis por assegurar o cumprimento das normas de protecção constantes do anexo I pelo CBP não assegurem convenientemente esse mesmo cumprimento.

3. Se a informação recolhida nos termos do artigo 3.º e dos n.os 1 e 2 do presente artigo demonstrar que os princípios básicos necessários a um nível adequado de protecção das pessoas singulares não estão a ser respeitados, ou que os organismos responsáveis por assegurar o cumprimento das normas de protecção pelo CBP não desempenham eficazmente as suas funções, o CBP deverá ser informado e, se necessário, o procedimento referido no n.º 2 do artigo 31.º da Directiva 95/46/CE será aplicado, com vista a revogar ou suspender a presente decisão.

Artigo 5.º

A aplicação da presente decisão será objecto de vigilância e quaisquer conclusões pertinentes serão comunicadas ao comité criado pelo artigo 31.º da Directiva 95/46/CE, nomeadamente todas as provas que possam afectar a afirmação do artigo 1.º da presente decisão, segundo a qual o nível de protecção dos dados pessoais contidos nos PNR dos passageiros transferidos para o CBP é adequado, nos termos do artigo 25.º da Directiva 95/46/CE.

Artigo 6.º

Os Estados-Membros tomarão todas as medidas necessárias para darem cumprimento à presente decisão no prazo de quatro meses a contar da data da sua notificação.

Artigo 7.º

A presente decisão expira três anos e seis meses após a data da sua notificação, a menos que seja prorrogada nos termos do procedimento estabelecido no n.º 2 do artigo 31.º da Directiva 95/46/CE.

Artigo 8.º

Os Estados-Membros são os destinatários da presente decisão.

Feito em Bruxelas, em 14 de Maio de 2004.

Pela Comissão

Frederik BOLKESTEIN

Membro da Comissão

ANEXO

DECLARAÇÃO DE COMPROMISSO DO «*DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION*» (CBP)

Em apoio da intenção da Comissão Europeia (Comissão) de exercer os poderes que lhe são conferidos pelo n.º 6 do artigo 25.º da Directiva 95/46/CE (a directiva) e de aprovar uma decisão reconhecendo que o *Bureau of Customs and Border Protection* (CBP: serviço responsável pelas alfândegas e pela protecção das fronteiras) do *Department of Homeland Security* (DHS: Ministério norte-americano da Segurança Interna) fornece um nível de protecção adequado para efeitos de transferência, pelas companhias aéreas, de dados dos registos identificadores de passageiros (PNR: *Passenger Name Records*) [1] abrangidos pelo âmbito de aplicação da directiva, o CBP assume os seguintes compromissos:

Fundamentos jurídicos para a obtenção de PNR

1. Nos termos da lei [título 49, *United States Code*, secção 44909(c)(3)] e dos seus regulamentos de aplicação (provisórios) (título 19, *Code of Federal Regulations*, secção 122.49b), todas as companhias aéreas que efectuem voos internacionais de passageiros com destino a ou provenientes dos Estados Unidos devem possibilitar ao CBP (antigo *Customs Service* — serviço norte americano das alfândegas) o acesso electrónico aos dados dos PNR que estejam compilados e armazenados nos sistemas automatizados de reserva/controlo das partidas da companhia aérea («sistemas de reserva»).

Utilização dos dados dos PNR pelo CBP

2. Na sua maior parte, os elementos contidos nos dados dos PNR podem ser obtidos pelo CBP através do exame do bilhete de avião e demais documentos de viagem de um determinado passageiro, em conformidade com as suas normais atribuições de controlo das fronteiras, mas a possibilidade de receber estes dados por via electrónica permitirá ao CBP facilitar consideravelmente as viagens de boa fé e levar a cabo uma avaliação atempada, eficaz e eficiente dos riscos apresentados pelos passageiros.

3. Os dados dos PNR são utilizados pelo CBP estritamente para impedir e combater 1. o terrorismo e crimes conexos; 2. outros crimes graves, incluindo o crime organizado, que são, por natureza, transnacionais; e 3. a fuga a mandados judiciais ou à detenção pelos crimes atrás descritos. A utilização de dados dos PNR para estes efeitos permite ao CBP concentrar os seus recursos nas situações de elevado risco, facilitando e salvaguardando assim as viagens de boa-fé.

Exigências relativas aos dados

4. Os dados requeridos pelo CBP estão listados no anexo A do presente documento. (Esses elementos identificados são doravante referidos como «PNR» na presente declaração de compromisso.) Embora o CBP requeira acesso a cada um dos 34 elementos listados no anexo A, considera que só raramente um PNR individual incluirá um conjunto completo de todos os dados identificados. Nos casos em que o PNR não inclua um conjunto completo de todos os dados identificados, o CBP não procurará obter acesso directo, a partir do sistema de reservas da companhia aérea, a outros dados do PNR que não estejam listados no anexo A.

5. Quanto aos dados identificados como «OSI» e «SSI/SSR» (geralmente referidos como observações gerais e campos abertos), o sistema automático do CBP irá pesquisar nesses campos quaisquer outros dados identificados no anexo A. O pessoal do CBP não está autorizado a percorrer manualmente todos os campos OSI e SSI/SSR, a menos que o indivíduo que é objecto do PNR tenha sido identificado pelo CBP como apresentando um elevado risco em relação a qualquer dos objectivos referidos no n.º 3.

6. As informações pessoais adicionais pesquisadas em resultado directo dos dados do PNR serão obtidas de fontes externas à administração central, apenas pelos canais legais, incluindo os canais de auxílio judiciário mútuo sempre que apropriado, e unicamente para os objectivos definidos no n.º 3 da presente declaração de compromisso. Por exemplo, se o número de um cartão de crédito figura num PNR, as informações relativas às transacções relacionadas com a conta bancária correspondente podem ser obtidas no quadro de um procedimento legal, como uma intimação (*subpoena*) emitida por um grande júri, um mandado judicial ou qualquer outra forma prevista por lei. Além disso, o acesso aos registos relacionados com as contas de correio electrónico decorrentes de um PNR fica sujeito às normas legais dos Estados Unidos em matéria de intimações (*subpoenas*), mandados judiciais, mandados de prisão (*warrants*) e outros procedimentos legais, dependendo do tipo de informação que se pretenda obter.

7. O CBP consultará a Comissão Europeia quanto à revisão dos dados pretendidos dos PNR (anexo A) antes de proceder a essa revisão, se tiver conhecimento de campos adicionais de PNR que as companhias aéreas possam ter acrescentado aos seus sistemas e que sejam susceptíveis de melhorar consideravelmente a capacidade de o CBP efectuar avaliações dos riscos apresentados pelos passageiros, ou se as circunstâncias indicarem que um campo PNR anteriormente não requerido é necessário para cumprir os objectivos específicos referidos no n.º 3 da presente declaração de compromisso.

[1] Para efeitos da presente declaração de compromisso, os termos «passageiro» e «passageiros» incluem igualmente os membros da tripulação.

8. O CBP pode transferir PNR em bloco para a *Transportation Security Administration* (TSA), para que esta entidade possa testar o seu sistema informatizado de pré-selecção dos passageiros (*Computer Assisted Passenger Prescreening System II*, ou CAPPS II). Essas transferências não se efectuarão sem que, primeiro, se autorize que os dados dos PNR dos voos domésticos dos Estados Unidos sejam utilizados para os testes. Os dados dos PNR transferidos ao abrigo desta disposição não serão conservados pela TSA ou por quaisquer outros participantes directamente envolvidas nos testes para além do período necessário para os efectuar, nem serão transferidos para terceiros [2]. O objectivo das transferências é estritamente o de testar o sistema e as interfaces CAPPS II e, excepto em situações de emergência que envolvam a clara identificação de um conhecido terrorista ou de um indivíduo com ligações comprovadas a actos terroristas, não terão quaisquer consequências operacionais. Nos termos da disposição que requer um método automático de filtragem dos dados, descrito no n.º 10, o CBP terá filtrado e apagado dados «sensíveis» antes de transferir quaisquer PNR em bloco para a TSA ao abrigo da presente disposição.

Tratamento de dados «sensíveis»

9. O CBP não utilizará dados «sensíveis» (ou seja, dados pessoais que especifiquem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, pertença a sindicatos, situação médica ou de saúde, ou orientação sexual da pessoa em questão) do PNR, tal como abaixo se descreve.

10. O CBP irá concretizar, com a maior brevidade possível, um sistema automatizado para filtrar e apagar certos códigos e termos «sensíveis» dos PNR, identificados em colaboração com a Comissão Europeia.

11. Até à concretização desses filtros automáticos, o CBP declara que não utiliza nem utilizará dados «sensíveis» dos PNR e compromete se-a apagar tais dados de qualquer divulgação discricionária de PNR, nos termos dos n.ºs 28 a 34 [3].

Método de acesso aos dados dos PNR

12. Quanto aos dados dos PNR a que o CBP acede (ou que o CBP recebe) directamente a partir dos sistemas de reserva das companhias aéreas para efeitos de identificação dos indivíduos susceptíveis de serem submetidos a controlos nas fronteiras, o pessoal do CBP apenas terá acesso (ou receberá) e poderá utilizar dados dos PNR relativos a pessoas cujas viagens compreendam um voo destinado a ou proveniente [4] dos Estados Unidos.

13. O CBP «extrairá» as informações relativas aos passageiros dos sistemas de reserva das companhias aéreas até ao momento em que estas estejam em condições de concretizar um sistema de «exportação» dos dados para o CBP.

14. O CBP extrairá os dados dos PNR relativos a um determinado voo o mais tardar 72 horas antes da sua partida e verificará novamente os sistemas no máximo três vezes entre a extracção inicial, a descolagem do voo de um aeroporto estrangeiro e a sua chegada aos Estados Unidos, ou entre a extracção inicial e a partida do voo dos Estados Unidos, conforme o caso, a fim de detectar qualquer alteração dos dados. Na eventualidade de as companhias aéreas estarem dotadas de um sistema automático de exportação dos dados dos PNR, o CBP necessita de receber os dados 72 horas antes da descolagem do voo, desde que qualquer alteração dos dados dos PNR efectuada entre esse momento e a hora de chegada aos Estados Unidos ou de partida deste país seja igualmente transmitida ao CBP [5]. No caso — pouco habitual — de o CBP obter antecipadamente dados que indiquem que indivíduo(s) suscitando preocupações particulares pode(m) viajar a bordo de um voo destinado a ou proveniente dos Estados Unidos, ou que atravesse esse país, o CBP pode extrair (ou solicitar a exportação especial) de dados dos PNR com uma antecedência superior a 72 horas antes da partida do voo, para garantir a tomada de medidas adequadas, quando tal for essencial para impedir ou combater uma das infracções referidas no n.º 3. Na medida do possível, nos casos em que o CBP tenha de aceder aos dados dos PNR com uma antecedência superior a 72 horas antes da partida do voo, seguirá os procedimentos habituais de aplicação da lei.

---

[2] Para efeitos desta disposição, o CBP não é considerado nem como participante directamente envolvida no processo de teste CAPPS II, nem como um terceiro.

[3] Antes da concretização dos filtros automáticos pelo CBP (mencionada no n.º 10), se existirem dados «sensíveis» num PNR divulgado de forma não discricionária pelo CBP, tal como se refere no n.º 35, o CBP envidará todos os esforços para limitar a divulgação destes dados «sensíveis», nos termos da legislação norte-americana.

[4] Isto inclui as pessoas em trânsito nos Estados Unidos.

[5] Caso as companhias aéreas concordem em exportar os dados dos PNR para o CBP, este encetará negociações com elas quanto à possibilidade de exportar os dados dos PNR a intervalos regulares entre 72 horas antes da partida do voo de um aeroporto estrangeiro e a sua chegada aos Estados Unidos, ou dentro de 72 horas antes da partida do voo dos Estados Unidos, conforme o caso. O CBP utilizará um método de exportação dos dados dos PNR necessários que satisfaça as suas necessidades de efectuar uma avaliação eficaz dos riscos e, simultaneamente, minimize o impacto económico sobre as companhias aéreas.

Armazenamento de dados dos PNR

15. Se tal for aprovado pela administração nacional dos arquivos e registos (*National Archives and Records Administration*) (44 U.S.C. 2101, e seguintes), o CBP limitará o acesso em linha aos dados dos PNR aos utilizadores autorizados do CBP [6] e a um período de sete dias, após o qual o número de funcionários autorizados a aceder aos dados dos PNR será novamente limitado, por um período de três anos e seis meses a contar da data de acesso aos dados (ou de recepção dos dados) fornecidos pelo sistema de reservas da companhia aérea. No final desse período de três anos e seis meses, os dados dos PNR que não tenham sido consultados manualmente durante esse lapso de tempo serão destruídos. Os dados dos PNR que tenham sido consultados manualmente no decurso do período inicial de três anos e seis meses serão transferidos pelo CBP para um ficheiro de registos apagados [7], no qual permanecerão por um período de oito anos antes de serem destruídos. Contudo, estes prazos não se aplicam aos dados dos PNR que estejam relacionados com um registo específico de medidas de aplicação (estes dados ficarão acessíveis até ao arquivamento deste registo). Quanto aos PNR a que o CBP acede (ou que o CBP recebe) directamente a partir do sistema de reservas da companhia aérea durante o período de vigência da presente declaração de compromisso, o CBP respeitará os princípios de conservação dos dados definidos na presente disposição, sem prejuízo da possível expiração da presente declaração de compromisso, nos termos do seu n.º 46.

Segurança do sistema informático do CBP

16. O pessoal autorizado do CBP tem acesso aos PNR por meio de um sistema intranet exclusivo, fechado e cifrado, cuja conexão é controlada pelo centro de dados das alfândegas (*Customs Data Center*). Os dados dos PNR armazenados na base de dados do CBP são acessíveis unicamente para consulta (*read only*) pelo pessoal autorizado, o que significa que os dados podem ser reformatados, mas não substancialmente alterados, seja de que forma for, pelo CBP a partir do momento em que este a eles tenha acesso através do sistema de reservas da companhia aérea.

17. Nenhum outro organismo estrangeiro, federal, estatal ou local dispõe de acesso electrónico directo aos dados dos PNR através das bases de dados do CBP (inclusivamente através do sistema integrado de controlo nas fronteiras — *Interagency Border Inspection System*, ou IBIS).

18. Os pormenores relativos ao acesso à informação contida nas bases de dados do CBP (como, por exemplo, quem, onde, quando — data e hora — e as eventuais revisões dos dados) são automaticamente registados e regularmente auditados pelo *Office of Internal Affairs* (Ministério dos Assuntos Internos), a fim de impedir qualquer utilização não autorizada do sistema.

19. Apenas podem aceder aos dados dos PNR determinados funcionários e empregados do CBP, ou subcontratados para as tecnologias da informação [8] (sob a supervisão do CBP), que tenham sido objecto de uma investigação quanto aos seus antecedentes, disponham de uma conta activa e protegida por senha (*password*) no sistema informático do CBP e tenham uma autorização oficial para examinar aqueles dados.

20. Os funcionários, empregados e subcontratados do CBP devem seguir, de dois em dois anos, uma formação em segurança e confidencialidade dos dados, sancionada por um exame. A auditoria do sistema do CBP tem por objectivo controlar e garantir o respeito do conjunto das exigências relativas à protecção da privacidade e à segurança dos dados.

21. Qualquer acesso não autorizado por um membro do pessoal do CBP aos sistemas de reservas das companhias aéreas ou ao sistema informático do CBP que contém os PNR é passível de medidas disciplinares severas (que podem incluir o despedimento) e de sanções penais (multas, prisão até um ano, ou mesmo ambas) (título 18, *United States Code*, secção 1030).

22. As políticas e os regulamentos do CBP prevêem igualmente medidas disciplinares severas (que podem incluir o despedimento) contra qualquer membro do pessoal deste organismo que divulgue informações contidas nos seus sistemas informáticos sem autorização oficial (título 19, *Code of Federal Regulations*, secção 103.34).

23. É passível de sanções penais (nomeadamente multas, prisão até um ano, ou mesmo ambas) qualquer funcionário ou empregado dos Estados Unidos que divulgue dados dos PNR obtidos no âmbito das suas funções, quando tal divulgação for proibida por lei (título 18, *United States Code*, secções 641, 1030 e 1905).

---

[6] Estes utilizadores autorizados do CBP incluem os funcionários afectados às unidades analíticas dos gabinetes locais, bem como os que estão afectados ao *National Targeting Center*. Tal como atrás se indica, as pessoas responsáveis pela manutenção, desenvolvimento ou auditoria da base de dados do CBP terão igualmente acesso a esses dados para esses fins específicos.

[7] Embora o registo dos PNR não seja tecnicamente apagado quando é transferido para o ficheiro de registos apagados, é armazenado sob a forma de dados em bruto (não numa forma directamente pesquisável, pelo que não tem utilidade para as investigações «tradicionais») e só é acessível ao pessoal autorizado do *Office of Internal Affairs* do CBP (e, em certos casos, do *Office of the Inspector General*, em relação com as auditorias), bem como ao pessoal responsável pela manutenção da base de dados do *Office of Information Technology* do CBP, exclusivamente em caso de necessidade.

[8] O acesso dos subcontratados a quaisquer dados dos PNR contidos nos sistemas informáticos do CBP fica limitado às pessoas que tiverem assinado com o CBP um contrato de assistência à manutenção ou desenvolvimento desses sistemas informáticos.

Tratamento e protecção dos dados dos PNR pelo CBP

24. O CBP considera os dados dos PNR, independentemente da nacionalidade ou do país de residência das pessoas em causa, como sensíveis e confidenciais, de carácter pessoal no caso do passageiro, ou como sendo do âmbito do sigilo comercial no caso da companhia aérea, pelo que não divulga estes dados ao público, com as excepções previstas na presente declaração de compromisso ou na lei.

25. A divulgação ao público de dados dos PNR é geralmente regulada pela lei relativa à liberdade da informação (*Freedom of Information Act*, ou FOIA) (título 5, *United States Code*, secção 552), que autoriza qualquer pessoa (independentemente da sua nacionalidade ou país de residência) a consultar os registos de uma agência federal americana, excepto se estes registos (ou parte deles) estiverem protegidos da divulgação por uma excepção prevista na lei FOIA. Entre as excepções previstas nesta lei, há uma que autoriza uma agência a impedir um registo (ou parte dele) de ser divulgado, se este contiver informações confidenciais de carácter comercial, se a divulgação for de molde a constituir uma violação claramente injustificada da privacidade, ou se as informações em causa tiverem sido compiladas para efeitos da aplicação da lei, na medida em que se possa razoavelmente pensar que essa divulgação constituiria uma violação injustificada da privacidade [título 5, *United States Code*, secções 552(b)(4), (6), (7)(C)].

26. Os regulamentos em vigor no CBP (título 19, *Code of Federal Regulations*, secção 103.12), que regem o processamento dos pedidos de informação (como dados dos PNR) em conformidade com a lei FOIA, prevêem especificamente que (com certas excepções limitadas, no caso de pedidos efectuados pelos titulares dos dados) as regras da lei FOIA em matéria de divulgação não são aplicáveis aos registos do CBP relativos: 1. às informações confidenciais de carácter comercial; 2. aos dados que envolvem a privacidade e cuja divulgação constituiria uma violação claramente injustificada da mesma; e 3. às informações compiladas para efeitos jurídicos, nos casos em que se possa razoavelmente pensar que a sua divulgação constituiria uma violação injustificada da privacidade [9].

27. No quadro de qualquer procedimento administrativo ou judicial decorrente de um pedido, apresentado ao abrigo da lei FOIA, de informações dos PNR obtidas a partir das companhias aéreas, o CBP invocará que, ao abrigo desta mesma lei, tais registos estão protegidos da divulgação.

Transferência de dados dos PNR para outras autoridades estatais

28. Com excepção das transferências entre o CBP e a TSA efectuadas nos termos do n.º 8 da presente declaração de compromisso, os serviços do Ministério da Segurança Interna (*Department of Homeland Security*, ou DHS) serão tratados como «organismos terceiros», sujeitos às mesmas regras e condições de acesso aos dados dos PNR que as outras entidades estatais exteriores àquele ministério.

29. O CBP apenas transmitirá, se assim o decidir e numa base casuística, dados dos PNR a outras autoridades estatais — incluindo estrangeiras — de luta contra o terrorismo, para efeitos de prevenção ou combate às infracções mencionadas no n.º 3 da presente declaração de compromisso (as autoridades com as quais o CBP pode compartilhar estes dados são doravante referidas como «autoridades designadas»).

30. O CBP exercerá de forma judiciosa o seu poder discricionário de transferir dados dos PNR para os efeitos declarados. Antes de mais, o CBP determinará se a razão para a divulgação dos dados dos PNR a outra autoridade designada se adequa aos objectivos previstos (ver o n.º 29 *supra*). Se for esse o caso, o CBP determinará se a autoridade designada é responsável pela prevenção, investigação ou prossecução criminal de violações ou por fazer valer ou concretizar um estatuto ou regulamento relacionado com esse objectivo, sempre que o CBP tenha conhecimento de uma indicação de violação ou potencial violação da lei. A fundamentação da divulgação terá de ser revista à luz de todas as circunstâncias apresentadas.

31. A fim de regular a divulgação de dados dos PNR que podem ser transmitidos às outras autoridades designadas, o CBP é considerado o «proprietário» dos dados e essas autoridades designadas ficam sujeitas, em virtude das condições expressas de divulgação, às seguintes obrigações: 1. utilizar os dados dos PNR unicamente para os fins previstos no n.º 29 ou no n.º 34 da presente declaração de compromisso, conforme o caso; 2. velar pela eliminação sistemática dos dados dos PNR recebidos, no respeito dos procedimentos de conservação de registos da autoridade designada; e 3. obter uma autorização expressa do CBP para qualquer divulgação posterior. O não cumprimento das condições de transferência pode dar azo a uma investigação e a um relatório do *Chief Privacy Officer* (director responsável pela confidencialidade) do DHS, o que poderá ter como consequência que a autoridade designada em questão possa vir a ficar privada do direito de receber do CBP transferências subsequentes de dados dos PNR.

[9] O CBP invocará estas excepções de maneira uniforme, independentemente da nacionalidade ou do país de residência do titular dos dados.

32. Qualquer divulgação de dados dos PNR pelo CBP é efectuada na condição de o organismo destinatário tratar os dados em questão como informações confidenciais de carácter comercial e sensíveis, ou como informações confidenciais de carácter pessoal para os passageiros, nos termos dos n.os 25 e 26, que há que considerar como protegidas da divulgação, nos termos da lei FOIA (5 U.S.C. 552). Além disso, o organismo destinatário será informado de que qualquer divulgação ulterior das informações em causa não é permitida sem a prévia autorização expressa do CBP. O CBP não autorizará qualquer transferência subsequente de dados dos PNR para objectivos diferentes dos previstos nos n.os 29, 34 ou 35 da presente declaração de compromisso.

33. Os membros do pessoal das autoridades designadas que divulguem dados dos PNR sem autorização adequada são passíveis de sanções penais (título 18, *United States Code*, secções 641, 1030 e 1905).

34. Nenhuma disposição da presente declaração de compromisso pode impedir a utilização ou a divulgação de dados dos PNR às autoridades estatais competentes, quando tal divulgação for essencial para a protecção dos interesses vitais do titular dos dados ou de outras pessoas, nomeadamente no caso de riscos sanitários graves. As divulgações efectuadas para estes fins estão sujeitas às mesmas condições que as aplicáveis às transferências descritas nos n.os 31 e 32.

35. Nenhuma disposição da presente declaração de compromisso pode impedir a utilização ou a divulgação de dados dos PNR no âmbito de um processo penal ou ao abrigo de outras exigências previstas por lei. O CBP informará a Comissão Europeia da adopção, pelas autoridades norte-americanas, de qualquer legislação com incidência sobre a substância das disposições da presente declaração de compromisso.

Informação, acesso aos dados e vias de recurso para os titulares dos dados dos PNR

36. O CBP dará conhecimento aos passageiros das exigências relativas aos PNR e das questões ligadas à sua utilização (ou seja, informação geral relativa à entidade responsável pela recolha dos dados, finalidade dessa recolha, protecção dos dados, partilha dos dados, identidade do funcionário responsável, vias de recurso disponíveis e pontos de contacto para apresentação de perguntas ou problemas, etc., para publicação no *site* do CBP, em brochuras de viagem, etc.).

37. Os pedidos apresentados pelos titulares dos dados (também conhecidos por «primeiros requerentes») de cópias de dados dos PNR contidos nas bases de dados do CBP relativos a esses titulares são tratados em conformidade com a lei FOIA. Esses pedidos podem ser enviados pelo correio para: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229; ou entregues pessoalmente a: Disclosure Law Officer, U.S. Customs and Border Protection, Headquarters, Washington, D.C. Mais informações sobre os procedimentos de apresentação de pedidos ao abrigo da lei FOIA constam da secção 103.5 do título 19 do *U.S. Code of Federal Regulations*. No caso de pedidos apresentados pelos próprios titulares dos dados, o facto de o CBP normalmente considerar os dados dos PNR como informações confidenciais de carácter pessoal, no caso dos passageiros, ou informações abrangidas pelo segredo comercial, no caso das companhias aéreas, não será invocado pelo CBP como motivo para não comunicar os dados dos PNR às pessoas em questão, ao abrigo da lei FOIA.

38. Em certas circunstâncias excepcionais, o CBP pode fazer uso da faculdade que lhe é conferida pela lei FOIA de recusar ou adiar a divulgação da totalidade (ou, mais provavelmente, de parte) de um PNR a um primeiro requerente, em conformidade com o título 5, secção 552(b) do *United States Code* (por exemplo, «se se puder razoavelmente considerar que a divulgação ao abrigo da lei FOIA é de molde a obstruir um processo de execução» ou «se forem divulgadas técnicas e procedimentos das investigações judiciais (…), com o risco provável de permitir que a lei seja contornada»). Segundo a lei FOIA, qualquer requerente pode contestar, por meio de recurso administrativo ou judicial, a decisão do CBP de não comunicar informações [ver 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7 103.9].

39. O CBP compromete-se a rectificar dados [10], a pedido dos passageiros, membros da tripulação, companhias aéreas ou autoridades responsáveis pela protecção dos dados (APD) dos Estados-Membros da UE (desde que essa rectificação seja especificamente autorizada pelo titular dos dados), nos casos em que estabelecer que tais dados figuram na sua base de dados e considerar que uma correcção é justificada e adequadamente fundamentada. O CBP informará a autoridade designada que tenha recebido os dados dos PNR em questão de qualquer rectificação concreta desses dados.

[10] Ao utilizar o termo «rectificar», o CBP pretende deixar claro que não está autorizado a modificar os dados dos PNR a que tem acesso através das companhias aéreas. Será criado um registo separado ligado ao PNR para mencionar que os dados estavam incorrectos e introduzir a correspondente correcção. Mais especificamente, o CBP inscreverá no registo de exame secundário do passageiro (*passenger's secondary examination record*) uma menção assinalando que certos dados do PNR podem ser ou são inexactos.

40. Os pedidos de rectificação de dados dos PNR contidos na base de dados do CBP e as queixas individuais apresentadas por titulares desses dados quanto ao tratamento que lhes tenha sido dado pelo CBP devem ser enviados, quer directamente, quer através da APD competente (desde que o titular dos dados tenha dado o seu consentimento expresso) para o seguinte endereço: Assistant Commissioner, Office of Field Operations, U.S. Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

41. Sempre que uma queixa não puder ser resolvida pelo CBP, pode ser enviada, por escrito, para o *Chief Privacy Officer*, Department of Homeland Security, Washington, DC 20528, que examinará a situação e tentará dirimir o litígio ([11]).

42. Além disso, o *Privacy Office* do DHS examinará com urgência as queixas que lhe sejam remetidas pelas APD dos Estados-Membros da União Europeia em nome de um residente da UE, desde que este residente tenha autorizado essas autoridades a agir em seu nome e considere que a sua queixa em matéria de protecção dos dados dos PNR não foi adequadamente tratada pelo CBP (em conformidade com os n.os 37 a 41 da presente declaração de compromisso) ou pelo *Privacy Office* do DHS. Este último comunicará as suas conclusões e aconselhará a(s) APD(s) quanto às medidas tomadas, se for esse o caso. O *Chief Privacy Officer* (director) do DHS fará referência, no seu relatório ao Congresso norte-americano, a informações quanto ao número, ao teor e à resolução das queixas relativas ao processamento dos dados de carácter pessoal como os dos PNR ([12]).

Cumprimento das disposições

43. O CBP compromete-se, juntamente com o DHS, a efectuar, uma vez por ano ou mais frequentemente, consoante decisão das partes, uma revisão conjunta com a Comissão Europeia, assistida, eventualmente, por representantes das autoridades comunitárias responsáveis pela aplicação da lei e/ou das autoridades dos Estados-Membros da União Europeia ([13]), da execução da presente declaração de compromisso, a fim de contribuírem mutuamente para o bom funcionamento dos processos nela descritos.

44. O CBP aprovará os regulamentos, as directivas ou quaisquer outros diplomas que integrem as presentes disposições, a fim de garantir o cumprimento da presente declaração de compromisso pelos seus funcionários, empregados e subcontratados. Como já foi mencionado, o não cumprimento, por esses funcionários, empregados ou subcontratados, das regras estabelecidas por estes documentos pode implicar medidas disciplinares severas, ou mesmo sanções penais, conforme o caso.

Reciprocidade

45. Caso seja concretizado na União Europeia um sistema de identificação dos passageiros das companhias aéreas semelhante ao da Administração dos Estados Unidos, que obrigue as companhias aéreas a proporcionar às autoridades acesso aos dados dos PNR dos passageiros cuja viagem em curso inclua um voo com destino a ou partida da União Europeia, o CBP, estritamente na base da reciprocidade, incentivará as companhias aéreas com sede nos Estados Unidos a cooperar.

Revisão e expiração da declaração de compromisso

46. A presente declaração de compromisso é aplicável por um período de três anos e seis meses a contar da data da entrada em vigor de um acordo entre os Estados Unidos e a Comunidade Europeia autorizando o tratamento de dados dos PNR pelas companhias aéreas e sua transferência para o CBP, em conformidade com a directiva. Após dois anos e meio de vigência da presente declaração de compromisso, o CBP, juntamente com o DHS, encetará discussões com a Comissão no intuito de prorrogar a presente declaração de compromisso e quaisquer eventuais disposições conexas, em condições aceitáveis para ambas as partes. Se não for possível celebrar um acordo aceitável para ambas as partes antes da expiração da presente declaração de compromisso, esta deixará de produzir efeito.

([11]) O *Chief Privacy Officer* (director) do DHS é independente de qualquer direcção do DHS (*Department of Homeland Security*) e está estatutariamente obrigado a garantir que os dados pessoais sejam utilizados de maneira conforme com as leis aplicáveis na matéria (ver nota de pé-de-página 13). As decisões do *Chief Privacy Officer* são vinculativas para o DHS e não podem ser anuladas por motivos políticos.

([12]) Nos termos da secção 222 do *Homeland Security* Act de 2002 («a lei») (*Public Law* 107 296, datada de 25 de Novembro de 2002), o *Privacy Officer* for DHS está encarregue de efectuar uma «avaliação do impacto sobre a privacidade» das regras propostas por este ministério em matéria de «privacidade de dados pessoais, incluindo o tipo de dados pessoais recolhidos e o número de pessoas afectadas» e de apresentar relatórios anuais ao Congresso sobre «as actividades do ministério que afectam a privacidade …». A secção 222(5) da lei também incumbe expressamente o *Privacy Officer* do DHS de receber e comunicar ao Congresso «todas as queixas relativas à violação da privacidade».

([13]) As partes comunicarão uma à outra a composição das respectivas equipas e podem incluir autoridades competentes em matéria de privacidade/protecção de dados, controlo aduaneiro e outras formas de aplicação da lei, segurança das fronteiras e/ou segurança da aviação. As autoridades participantes ficarão obrigadas a estar na posse das autorizações necessárias e a respeitar a confidencialidade dos debates e da documentação a que poderão ter acesso. Todavia, a confidencialidade não invalidará que ambas as partes apresentem um relatório apropriado sobre os resultados da revisão conjunta às respectivas autoridades competentes, incluindo o Congresso americano e o Parlamento Europeu. Todavia, as autoridades participantes não podem, em caso algum, divulgar quaisquer dados pessoais de um titular de dados; também não podem divulgar quaisquer informações não públicas retiradas de documentos a que tenham acesso, nem quaisquer dados operacionais ou internos das agências aos quais tenham acesso no quadro da revisão conjunta. As partes determinarão conjuntamente as modalidades pormenorizadas da revisão conjunta.

Não criação de direito privado ou de precedente

47. A presente declaração de compromisso não cria nem confere qualquer direito ou benefício a qualquer pessoa ou parte, quer privada quer pública.

48. As disposições da presente declaração de compromisso não constituem um precedente para quaisquer negociações posteriores com a Comissão Europeia, a União Europeia, qualquer entidade conexa ou qualquer Estado terceiro em matéria de transferência de qualquer tipo de dados.

11 de Maio de 2004

ANEXO «A»

Dados dos PNR solicitados pelo CBP às companhias aéreas

1. Código localizador do PNR
2. Data da reserva
3. Data(s) prevista(s) da viagem
4. Nome
5. Outros nomes que figuram no PNR
6. Endereço
7. Todas as formas de informação sobre o pagamento
8. Endereço de facturação
9. Números de telefone de contacto
10. Itinerário completo para o PNR em questão
11. Informação sobre passageiros frequentes [limitada a milhas voadas e endereço(s)]
12. Agência de viagens
13. Agente de viagens
14. Informações do PNR sobre a divisão de códigos
15. Estatuto de viagem do passageiro *(Travel status)*
16. Informação do PNR separada/dividida
17. Endereço electrónico
18. Informações sobre a emissão dos bilhetes
19. Observações gerais
20 Número do bilhete
21. Número do lugar
22. Data da emissão do bilhete
23. Relato de não comparência
24. Números das etiquetas das bagagens
25. Passageiro de último minuto sem reserva *(Go show information)*
26. Informação OSI
27. Informação SSI/SSR
28. Informações sobre a fonte
29. Todas as alterações introduzidas no PNR
30. Número de passageiros no PNR
31. Informações sobre o lugar
32. Bilhetes só de ida
33. Informações APIS *(Advanced Passenger Information System)* eventualmente recolhidas
34. Campos ATFQ *(Automatic Ticketing Fare Quote)*