II

(Actes dont la publication n'est pas une condition de leur applicabilité)

COMMISSION

DÉCISION DE LA COMMISSION

du 14 mai 2004

relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique

[notifiée sous le numéro C(2004) 1914]

(Texte présentant de l'intérêt pour l'EEE)

(2004/535/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté européenne,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1], et notamment son article 25, paragraphe 6,

considérant ce qui suit:

(1) En vertu de la directive 95/46/CE, les États membres prévoient que le transfert de données à caractère personnel vers un pays tiers ne peut être effectué que si le pays tiers en question assure un niveau de protection adéquat et si les lois nationales de mise en application d'autres dispositions de la directive sont respectées avant le transfert.

(2) La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat. Sur la base de ce constat, des données à caractère personnel peuvent être transférées à partir des États membres sans qu'aucune garantie supplémentaire ne soit nécessaire.

(3) En vertu de la directive 95/46/CE, le niveau de protection des données est apprécié au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et par rapport à certaines conditions, énumérées à son article 25, paragraphe 2.

(4) Dans le cadre des transports aériens, le dossier passager (*Passenger Name Record*, ci-après dénommé le «PNR») est un fichier contenant les renseignements relatifs au voyage de chaque passager. Il renferme toutes les informations nécessaires au traitement et au contrôle des réservations par les compagnies aériennes contractantes ou partenaires. Aux fins de la présente décision, les termes «passager» et «passagers» incluent les «membres de l'équipage». «Compagnie aérienne contractante» signifie la compagnie auprès de laquelle le passager a réalisé sa première réservation ou auprès de laquelle des réservations additionnelles ont été réalisées après le commencement du voyage. «Compagnie aérienne partenaire» signifie toute compagnie aérienne auprès de laquelle la compagnie aérienne contractante a sollicité une place, sur un ou plusieurs de ses vols, pour un passager.

(5) Le Bureau des douanes et de la protection des frontières des États-Unis (*United States Bureau of Customs and Border Protection*, ci-après dénommé le «CBP») du ministère de la sécurité intérieure (*Department of Homeland Security*) exige de toutes les compagnies aériennes assurant un service international de transport de passagers à destination ou au départ des États-Unis qu'elles lui fournissent un accès électronique aux dossiers PNR recueillis et stockés dans leurs systèmes informatisés de réservation.

(6) Les exigences de transfert des données à caractère personnel contenues dans les PNR des passagers aériens vers le CBP se fondent sur une loi promulguée par les États-Unis en novembre 2001 [2] et sur des règlements de mise en œuvre adoptés par le CBP en vertu de cette loi [3].

[1] JO L 281 du 23.11.1995, p. 31. Directive modifiée par le règlement (CE) nº 1882/2003 (JO L 284 du 31.10.2003, p. 1).

[2] Titre 49, section 44909(c)(3), du code des États-Unis.

[3] Titre 19, section 122.49b, du code des règlements fédéraux.

(7) La législation américaine en question concerne le renforcement de la sécurité ainsi que les conditions d'entrée aux États-Unis et de sortie dudit pays. Sur ces points, les États-Unis ont un pouvoir de décision souverain dans le cadre de leur juridiction. Par ailleurs, les exigences ne sont pas contraires à leurs autres engagements internationaux. Les États-Unis sont un pays démocratique, gouverné par des principes de droit et doté d'une solide tradition en matière de libertés civiques. La légitimité de leur processus législatif ainsi que la force et l'indépendance de leur appareil judiciaire ne sont pas mises en question. La liberté de la presse constitue une autre garantie solide contre toute violation des libertés civiques.

(8) La Communauté soutient entièrement les États-Unis dans leur lutte contre le terrorisme, dans les limites imposées par le droit de la Communauté. La législation communautaire prévoit un dispositif qui permet d'établir un équilibre entre les exigences de sécurité et la sauvegarde de la vie privée. Par exemple, l'article 13 de la directive 95/46/CE permet aux États membres de prendre des mesures législatives visant à limiter la portée d'autres exigences visées dans la directive lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales.

(9) Les transferts de données concernent des responsables du traitement spécifiques, à savoir les compagnies aériennes assurant des liaisons entre la Communauté et les États-Unis et un seul destinataire aux États-Unis, à savoir le CBP.

(10) Tout arrangement visant à établir un cadre réglementaire pour les transferts de PNR aux États-Unis, notamment par le biais de la présente décision, doit être limité dans le temps. Une période de trois ans et demi a été convenue. Au cours de ce laps de temps, le contexte peut considérablement changer et la Communauté et les États-Unis conviennent qu'une révision des arrangements sera nécessaire.

(11) Le traitement par le CBP des données à caractère personnel contenues dans les PNR des passagers aériens qui lui sont transférés est régi par les dispositions figurant dans la «Déclaration d'engagement du Bureau des douanes et de la protection des frontières du ministère de la sécurité intérieure du 11 mai 2004» (ci-après dénommée «la déclaration d'engagement») et par la législation américaine dans les conditions prévues par la déclaration d'engagement.

(12) S'agissant de la législation américaine, la loi sur la liberté de l'information (*Freedom of Information Act*) est déterminante dans le contexte actuel dans la mesure où elle règle les conditions dans lesquelles le CBP peut s'opposer à des demandes de divulgation et traiter ainsi les PNR de manière confidentielle. Elle réglemente en outre la divulgation des PNR aux personnes concernées, qui est étroitement liée au droit d'accès dont celles-ci disposent. La loi sur la liberté de l'information s'applique sans distinction aux citoyens américains et étrangers.

(13) En ce qui concerne la déclaration d'engagement, et conformément à ce que prévoit son paragraphe 44, les dispositions de la déclaration d'engagement seront ou sont déjà incluses dans les textes de lois, règlements, directives ou autres instruments de politique des États-Unis et ont donc un effet juridique à des degrés divers. La déclaration d'engagement est publiée dans son intégralité dans le registre fédéral, sous la responsabilité du ministère de la sécurité intérieure. Elle représente donc un engagement politique sérieux et réfléchi de la part dudit ministère et son respect est contrôlé conjointement par les États-Unis et la Communauté. Les manquements peuvent être combattus le cas échéant par des moyens juridiques, administratifs et politiques. Leur répétition entraîne la suspension des effets de la présente décision.

(14) Les normes en vertu desquelles le CBP traite les données PNR des passagers sur la base de la législation américaine et de la déclaration d'engagement respectent les principes essentiels nécessaires pour assurer un niveau de protection adéquat des personnes physiques.

(15) En ce qui concerne le principe de limitation à une finalité spécifique, les données à caractère personnel des passagers aériens contenues dans les PNR qui sont transférés au CBP doivent être traitées dans un but spécifique et n'être utilisées ou communiquées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du transfert. En particulier, les données des PNR doivent être utilisées dans le but unique de prévenir et de combattre le terrorisme et les crimes liés au terrorisme, d'autres crimes graves, y compris la criminalité organisée, qui, par nature, revêtent un caractère transnational et la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés.

(16) En ce qui concerne la qualité des données et le principe de proportionnalité, qui doivent être considérés conjointement avec les motifs d'intérêt public importants justifiant le transfert des données des PNR, les données fournies au CBP ne doivent pas être ultérieurement modifiées par ce dernier. Un maximum de trente-quatre catégories de données des PNR sont transférées et les autorités américaines sont tenues de consulter la Commission avant l'ajout de toute nouvelle exigence. Les informations personnelles supplémentaires recherchées par suite directe de l'examen de données de PNR sont obtenues de sources non gouvernementales, uniquement par des moyens légaux. En règle générale, les PNR sont effacés après une période maximale fixée à trois ans et six mois, à l'exception des données consultées dans le cadre d'investigations spécifiques ou bien manuellement.

(17) En ce qui concerne le principe de transparence, le CBP informe les voyageurs sur la finalité du transfert et du traitement et leur fournit l'identité du responsable du traitement des données dans le pays tiers ainsi que d'autres renseignements.

(18) En ce qui concerne le principe de sécurité, le CBP prend les mesures de sécurité techniques et organisationnelles appropriées aux risques présentés par le traitement.

(19) Les droits d'accès et de rectification sont reconnus, dans la mesure où les personnes concernées peuvent demander une copie de leurs données PNR ainsi qu'une rectification des données inexactes. Les exceptions prévues sont dans l'ensemble comparables aux restrictions qui peuvent être imposées par un État membre au titre de l'article 13 de la directive 95/46/CE.

(20) Les transferts ultérieurs sont effectués, au cas par cas, vers d'autres agences gouvernementales, y compris les agences gouvernementales étrangères, chargées de la lutte contre le terrorisme ou de l'application de la loi, à des finalités correspondant à celles établies dans la déclaration de limitation de l'objectif. Des transferts pourront également être effectués pour la protection des intérêts vitaux de la personne concernée ou d'autres personnes, notamment en cas de risques sanitaires importants, ou dans le cadre d'une procédure pénale ou au titre d'autres exigences prévues par la loi. Ces agences doivent, en vertu des conditions expresses de diffusion, employer les données uniquement aux fins prévues et ne pas procéder à un transfert ultérieur sans l'accord du CBP. Aucune autre agence étrangère, fédérale, étatique ou locale ne dispose d'un accès électronique direct aux données de PNR *via* les bases de données du CBP. Le CBP s'oppose à la divulgation publique des PNR en vertu des exemptions prévues par les dispositions pertinentes de la loi sur la liberté de l'information.

(21) Le CBP n'utilise pas de données sensibles au sens de l'article 8 de la directive 95/46/CE et, en attendant la mise en place d'un système de filtrage permettant d'exclure de telles données des PNR transférés, il s'engage à mettre en œuvre les moyens de les effacer et de ne pas les utiliser dans l'intervalle.

(22) En ce qui concerne les mécanismes de mise en œuvre visant à garantir le respect de ces principes par le CBP, il est prévu un système de formation et d'information du personnel du CBP, ainsi que de sanctions pour les membres individuels dudit personnel. Le haut responsable de la protection de la vie privée (*Chief Privacy Officer*) auprès du ministère de la sécurité intérieure veille au respect par le CBP de la vie privée en général. Bien que fonctionnaire du ministère, il dispose d'une large autonomie organisationnelle et doit rendre compte chaque année au Congrès. Les personnes dont les données PNR ont été transférées peuvent adresser leurs plaintes au CBP ou, si elles ne sont pas résolues, au haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure, soit directement, soit par le biais des autorités chargées de la protection des données dans les États membres. Le Bureau de la protection de la vie privée du ministère de la sécurité intérieure examine en urgence les plaintes qui lui sont transmises par les autorités chargées de la protection des données dans les États membres au nom des résidents de la Communauté, si ceux-ci estiment que leurs plaintes n'ont pas été traitées de façon satisfaisante par le CBP ou le Bureau de la protection de la vie privée du ministère de la sécurité intérieure. Le respect de la déclaration d'engagement fait l'objet d'un examen annuel mené par le CBP, en conjonction avec ledit ministère, et une équipe dirigée par la Commission.

(23) Afin de contribuer à la transparence et en vue de garantir la capacité des autorités compétentes au sein des États membres d'assurer la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel, il convient de préciser les circonstances exceptionnelles dans lesquelles la suspension de flux particuliers de données peut être justifiée, indépendamment de la constatation du niveau de protection adéquat.

(24) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, a rendu plusieurs avis sur le niveau de protection assuré par les autorités américaines en ce qui concerne les données PNR. Ces avis ont guidé la Commission au cours de ses négociations avec le ministère de la sécurité intérieure. La Commission a pris note de ces avis lors de l'élaboration de la présente décision [1].

(25) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué par l'article 31, paragraphe 1, de la directive 95/46/CE,

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, le Bureau des douanes et de la protection des frontières des États-Unis (ci-après le «CBP») est considéré comme assurant un niveau de protection adéquat des données de dossiers passagers (ci-après dénommés les «PNR») transférées depuis la Communauté en ce qui concerne les vols à destination ou au départ des États-Unis, conformément à la déclaration d'engagement figurant en annexe.

Article 2

La présente décision concerne le niveau de protection adéquat assuré par le CBP en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive 95/46/CE et n'influe en rien sur d'autres conditions ou restrictions mettant en application d'autres dispositions de la directive qui s'appliquent au traitement de données à caractère personnel dans les États membres.

[1] Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis, adopté par le groupe de travail le 24.10.2002, disponible sur:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_fr.pdf
Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission de données passagers, adopté par le groupe de travail le 13 juin 2003, disponible sur:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_fr.pdf
Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP), adopté par le groupe de travail le 29 janvier 2004, disponible sur:
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_fr.pdf

Article 3

1. Sans préjudice des pouvoirs leur permettant de prendre des mesures pour assurer le respect des dispositions nationales adoptées conformément aux dispositions autres que l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent actuellement pour suspendre le transfert de données vers le CBP afin de protéger les personnes physiques à l'égard du traitement des données à caractère personnel qui les concernent dans l'un des deux cas suivants:

a) lorsqu'une autorité américaine compétente a constaté que le CBP ne respecte pas les normes applicables en matière de protection;

b) lorsqu'il est probable que les normes de protection établies en annexe ne sont pas respectées, qu'il y a tout lieu de croire que le CBP ne prend pas ou ne prendra pas, en temps voulu, les mesures qui s'imposent pour régler l'affaire en question, que la poursuite du transfert entraînerait un risque imminent de grave préjudice pour les personnes concernées et que les autorités compétentes de l'État membre se sont raisonnablement efforcées, dans ces circonstances, d'avertir le CBP et de lui donner la possibilité de répondre.

2. La suspension du transfert cesse dès que les normes de protection sont assurées et que les autorités compétentes dans les États membres concernés en sont averties.

Article 4

1. Les États membres informent sans tarder la Commission des mesures adoptées conformément à l'article 3.

2. Les États membres et la Commission s'informent aussi mutuellement de tout changement dans les normes de protection ainsi que des cas dans lesquels les mesures prises par les autorités chargées de veiller au respect par le CBP des normes de protection établies en annexe ne suffisent pas à en assurer le respect.

3. Si les informations recueillies conformément à l'article 3 et aux paragraphes 1 et 2 du présent article montrent que les principes essentiels nécessaires pour assurer un niveau de protection adéquat des personnes physiques ne sont plus respectés, ou qu'un quelconque organisme chargé de veiller au respect par le CBP des normes de protection établies en annexe ne remplit pas efficacement sa mission, le CBP sera informé et, si nécessaire, la procédure prévue à l'article 31, paragraphe 2, de la directive 95/46/CE sera applicable en vue d'annuler ou de suspendre la présente décision.

Article 5

La mise en œuvre de la présente décision sera évaluée et toute constatation pertinente sera rapportée au comité institué par l'article 31, de la directive 95/46/CE, et notamment de tout élément susceptible d'avoir une incidence sur l'appréciation, au titre de l'article 1er de la présente décision, du niveau de protection adéquat des données à caractère personnel contenues dans les PNR des passagers aériens transférés au CBP, au sens de l'article 25 de la directive 95/46/CE.

Article 6

Les États membres prennent toutes les mesures nécessaires pour se conformer à la présente décision dans les quatre mois à compter de sa notification.

Article 7

La présente décision vient à échéance trois ans et six mois à compter de sa notification, à moins qu'elle ne soit prolongée conformément à la procédure prévue à l'article 31, paragraphe 2, de la directive 95/46/CE.

Article 8

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 14 mai 2004.

Par la Commission

Frederik BOLKESTEIN

Membre de la Commission

ANNEXE

DÉCLARATION D'ENGAGEMENT DU BUREAU DES DOUANES ET DE LA PROTECTION DES FRONTIÈRES DU MINISTÈRE DE LA SÉCURITÉ INTÉRIEURE

Afin de soutenir le projet de la Commission européenne visant à exercer les pouvoirs qui lui sont conférés par l'article 25, paragraphe 6, de la directive 95/46/CE (ci-après dénommée la «directive») et à adopter une décision reconnaissant que le Bureau des douanes et de la protection des frontières (*Bureau of Customs and Border Protection*, ci-après le dénommé «CBP») du ministère de la sécurité intérieure (*Department of Homeland Security*) fournit un niveau de protection adéquat aux fins du transfert, par les compagnies aériennes, de données de dossiers passagers [1] (*Passenger Name Records*, ci-après dénommés les «PNR») susceptibles de relever du champ d'application de la directive, le CBP prend les engagements suivants.

Fondement juridique du droit d'obtention des PNR

1) En vertu de la loi [titre 49, section 44909(c)(3) du code des États-Unis] et de ses règlements (provisoires) de mise en œuvre (titre 19, section 122.49b du code des règlements fédéraux), toute compagnie aérienne assurant un service international de transport de passagers à destination ou au départ des États-Unis doit fournir au CBP un accès électronique aux données de PNR qui sont recueillies et stockées dans ses systèmes informatiques de réservation/contrôle des départs (ci-après dénommés les «systèmes de réservation»).

Utilisation des données de PNR par le CBP

2) Le CBP peut obtenir la plupart des éléments informatifs contenus dans les PNR en examinant le billet d'avion et les autres documents de voyage des passagers lors de l'exercice de son autorité normale de contrôle aux frontières, mais la possibilité de recevoir ces données par voie électronique lui permettra de faciliter considérablement le trafic passagers légitime et de mener de façon efficace une évaluation précoce des risques présentés par les passagers.

3) Le CBP utilise les données de PNR dans le but unique de prévenir et de combattre: 1) le terrorisme et les crimes liés au terrorisme; 2) d'autres crimes graves, y compris la criminalité organisée, qui, par nature, revêtent un caractère transnational, et 3) la fuite en cas de mandat d'arrêt ou de mise en détention pour l'un des crimes susmentionnés. L'utilisation de données de PNR à ces fins permet au CBP d'axer ses ressources sur des éléments à haut risque, facilitant et préservant ainsi le trafic passagers légitime.

Exigences relatives aux données

4) Les éléments informatifs requis par le CBP sont énumérés à l'annexe A. (Ces éléments identifiés sont appelés «PNR» aux fins de la présente déclaration d'engagement.) Bien que le CBP exige l'accès à chacune des trente-quatre rubriques énumérées à l'annexe A, il estime que les PNR individuels ne comprendront que rarement l'ensemble des données identifiées. Si le PNR ne comprend pas la totalité de ces rubriques, le CBP ne tentera pas d'accéder directement, via le système de réservation de la compagnie aérienne, à des données de PNR autres que celles citées à l'annexe A.

5) En ce qui concerne les rubriques «OSI» et «SSI/SSR» (communément qualifiées de remarques générales et de champs ouverts), le système informatique du CBP recherchera dans ces champs la présence d'autres éléments d'information énumérés à l'annexe A. Le personnel du CBP ne sera pas autorisé à parcourir manuellement la totalité des champs OSI et SSI/SSR, sauf si la personne faisant l'objet d'un PNR est considérée par le CBP comme présentant un risque élevé au regard de l'un des objectifs spécifiés au paragraphe 3.

6) Les informations personnelles supplémentaires qui seront recherchées par suite directe de l'examen de données de PNR seront obtenues de sources non gouvernementales, uniquement par des voies légales, y compris le cas échéant par le recours aux mécanismes d'entraide judiciaire, et seulement aux fins spécifiées au paragraphe 3. Par exemple, si un numéro de carte de crédit figure dans un PNR, des informations sur les opérations liées au compte bancaire concerné pourront être recherchées dans le cadre d'une procédure légale, comme une ordonnance de comparution (*subpoena*) prononcée par un grand jury, une ordonnance d'un tribunal, ou tout autre moyen légal. En outre, l'accès aux fichiers liés à des comptes de courrier électronique mentionnés dans un PNR obéira aux exigences de la loi des États-Unis en matière d'ordonnances de comparution (*subpoenas*), d'ordonnances des tribunaux, de mandats d'arrêt (*warrants*) et d'autres procédures légales, en fonction du type d'informations recherché.

7) Le CBP consultera la Commission au sujet de la révision de la liste des données de PNR requises figurant à l'annexe A avant de procéder à une telle révision, s'il vient à sa connaissance que les compagnies aériennes ont ajouté, dans leurs systèmes, des champs PNR qui faciliteraient grandement sa tâche d'évaluation des risques présentés par les passagers, ou s'il s'avère qu'un champ PNR auparavant non requis est nécessaire à la réalisation des objectifs précis spécifiés au paragraphe 3.

[1] Aux fins de la présente déclaration d'engagement, les termes «passager» et «passagers» incluent les membres d'équipage.

8) Le CBP est habilité à transmettre des séries de PNR à l'administration chargée de la sécurité des transports (*Transportation Security Administration*, ci-après la «TSA») afin de lui permettre de tester son système informatisé CAPPS II de contrôle précoce des passagers (*Computer Assisted Passenger Prescreening System II*). Il ne pourra être procédé à un tel transfert qu'à partir du moment où l'utilisation des données de PNR relatives à des vols intérieurs américains aux fins des essais du système aura été autorisée. Les données de PNR transférées en vertu de la présente disposition ne seront pas conservées par la TSA ni par aucune autre instance participant directement aux essais au-delà de la période nécessaire pour la réalisation de ceux-ci; elles ne seront pas non plus transmises à des tiers ([2]). La finalité du traitement est strictement limitée aux essais du système CAPPS II et de ses interfaces et, hormis dans des cas d'urgence où l'on procéderait à l'identification formelle d'un terroriste notoire ou d'un individu connu pour ses liens avec le terrorisme, un tel traitement n'aura pas de conséquences opérationnelles. Conformément au paragraphe 10 qui prévoit un système informatisé de filtrage des données, le CBP aura filtré et supprimé les données dites «sensibles» avant le transfert de séries de PNR à la TSA en vertu de la présente disposition.

Traitement des données «sensibles»

9) Le CBP n'utilisera pas de données «sensibles» figurant dans les PNR, à savoir des données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance à un syndicat ainsi que des données relatives à l'état de santé ou la vie sexuelle de la personne.

10) Le CBP mettra en œuvre, dans les délais les plus brefs, un système informatisé filtrant et supprimant des PNR certains codes et termes «sensibles» identifiés par le CBP après consultation de la Commission.

11) Dans l'attente de la mise en œuvre de ces filtres informatiques, le CBP affirme qu'il n'utilise et n'utilisera pas d'informations «sensibles» des PNR et s'engage à supprimer de telles données de toute divulgation discrétionnaire de PNR en vertu des paragraphes 28 à 34 ([3]).

Méthode d'accès aux données de PNR

12) En ce qui concerne les données de PNR auxquelles le CBP accède directement, ou qu'il reçoit directement, à partir des systèmes de réservation des compagnies aériennes afin d'identifier les individus susceptibles d'être soumis à un contrôle aux frontières, le personnel du CBP n'accédera aux données de PNR, ou ne recevra les données de PNR, et ne les utilisera que dans le cas de passagers dont le voyage comprend un vol à destination ou au départ ([4]) des États-Unis.

13) Le CBP «extraira» les informations relatives aux passagers des systèmes de réservation des compagnies aériennes jusqu'à ce que celles-ci soient en mesure de mettre en œuvre un système «exportant» les données concernées vers le CBP.

14) Le CBP extraira les données de PNR concernant un vol particulier au plus tôt 72 heures avant le départ de ce vol et vérifiera de nouveau les systèmes à trois reprises au maximum entre l'extraction initiale, le départ du vol d'un aéroport étranger et son arrivée aux États-Unis ou entre l'extraction initiale et le départ du vol des États-Unis, selon le cas, afin de relever toute modification des informations. Si les compagnies aériennes se dotent d'un système d'exportation des données de PNR, le CBP doit recevoir les données 72 heures avant le départ du vol, pour autant que toute modification des données de PNR effectuée entre ce moment et l'heure d'arrivée aux États-Unis ou de départ des États-Unis soit aussi transmise au CBP ([5]). Dans le cas inhabituel où le CBP obtiendrait à l'avance des informations indiquant qu'une ou des personnes suscitant des préoccupations particulières pourraient voyager sur un vol à destination ou au départ des États-Unis ou y faisant escale, le CBP pourrait extraire les données de PNR ou en solliciter une exportation spéciale avant le délai de 72 heures précédant le départ du vol afin de pouvoir prendre les mesures qu'il juge indispensables pour prévenir ou lutter contre un crime visé au paragraphe 3. Dans l'éventualité où le CBP devrait consulter des données de PNR avant le délai de 72 heures précédant le départ du vol, il utilisera, dans la mesure du possible, les procédures habituelles d'application de la loi.

([2]) Aux fins de la présente disposition, le CBP n'est considéré ni comme une instance participant directement aux essais du système CAPPS II, ni comme un organisme tiers.

([3]) Tant que les filtres informatisés visés au paragraphe 10 ne seront pas opérationnels, le CBP mettra tout en œuvre, dans le respect de la législation des États-Unis, pour éviter que des données «sensibles» de PNR soient rendues publiques lorsque de telles données figurent dans un PNR faisant l'objet d'une divulgation non discrétionnaire par le CBP conformément au paragraphe 35.

([4]) En ce compris les passagers transitant par les États-Unis.

([5]) Si les compagnies aériennes acceptent d'exporter les données de PNR vers le CBP, celui-ci examinera avec elles la possibilité de transmettre automatiquement les données requises à des intervalles réguliers durant une période comprise entre le délai de 72 heures précédant le départ du vol d'un aéroport étranger et son arrivée aux États-Unis ou dans les 72 heures précédant le départ du vol d'un aéroport américain, selon le cas. Le CBP entend utiliser une méthode d'exportation des données requises qui satisfasse à ses impératifs d'évaluation efficace des risques, tout en minimisant les frais pour les compagnies aériennes.

Stockage des données de PNR

15) Sous réserve de l'approbation par l'administration des archives nationales (National Archives and Records Administration) (titre 44, sections 2101, et suiv. du code des États-Unis), le CBP limitera l'accès en ligne des données de PNR aux utilisateurs habilités du CBP [6] pendant une période de sept jours, au terme de laquelle le nombre de fonctionnaires autorisés à consulter les données de PNR sera restreint davantage pendant une période de trois ans et six mois à compter de la date d'accès aux données dans le système de réservation de la compagnie aérienne (ou de la date de réception des données). Au terme de la période de trois ans et six mois, les données de PNR qui n'auront pas été consultées manuellement durant ce laps de temps seront détruites. Les données de PNR qui auront été consultés manuellement au cours de la période initiale de trois ans et six mois seront transférées par le CBP vers un fichier de dossiers supprimés [7], où elles seront conservées pendant une période de huit ans avant leur destruction. Ces délais ne s'appliqueraient toutefois pas aux données de PNR en rapport avec un dossier répressif spécifique. De telles données demeureraient accessibles jusqu'à ce que le dossier en question soit archivé. En ce qui concerne les PNR auxquels le CBP aura directement accès, ou qu'il recevra directement, par l'intermédiaire des systèmes de réservation des compagnies aériennes durant la période d'application des présents engagements, le CBP respectera les règles de conservation des données définies dans le présent paragraphe, sans préjudice de l'expiration possible de la période de validité de la présente déclaration d'engagement conformément au paragraphe 46.

Sécurité des systèmes informatiques du CBP

16) Le personnel habilité du CBP dispose d'un accès aux PNR par le biais du système intranet fermé et chiffré de bout en bout du CBP, la connexion étant contrôlée par le Centre de données des douanes (*Customs Data Center*). Les données de PNR stockées dans le système du CBP sont uniquement accessibles en «lecture seule» par le personnel habilité, ce qui signifie que, une fois ces données obtenues à partir du système de réservation d'une compagnie aérienne, elles pourront être reformatées par programme, mais leur contenu ne pourra pas être modifié de quelque manière que ce soit par le CBP.

17) Aucune autre agence étrangère, fédérale, étatique ou locale ne dispose d'un accès électronique direct aux données de PNR via les bases de données du CBP, y compris via le système inter-agences IBIS d'inspection aux frontières (*Interagency Border Inspection System*).

18) Les précisions concernant l'accès aux informations contenues dans les bases de données du CBP [du type qui, où, quand (date et heure) et les révisions éventuelles des données] sont automatiquement enregistrées et font l'objet d'un audit régulier par le Bureau des affaires internes (*Office of Internal Affairs*) afin d'empêcher toute utilisation non autorisée du système.

19) Seuls certains fonctionnaires, agents ou sous-traitants en technologies de l'information du CBP [8] sous la supervision de celui-ci, qui ont satisfait à une enquête concernant leurs antécédents, qui disposent d'un compte actif et protégé par mot de passe dans le système informatique du CBP et qui sont officiellement habilités à examiner les données de PNR, peuvent accéder aux données de PNR.

20) Les fonctionnaires, agents et sous-traitants du CBP sont tenus de suivre, tous les deux ans, une formation à la sécurité et à la confidentialité des données, sanctionnée par un examen. L'audit des systèmes du CBP a pour but de contrôler et de garantir le respect de l'ensemble des exigences relatives à la protection de la vie privée et à la sécurité des données.

21) Tout accès non autorisé par un membre du personnel du CBP aux systèmes de réservation des compagnies aériennes ou au système informatique du CBP contenant les PNR expose à des mesures disciplinaires sévères pouvant aboutir au licenciement et est passible de sanctions pénales telles que des amendes, un emprisonnement allant jusqu'à un an, voire les deux (titre 18, section 1030, du code des États-Unis).

22) Les lignes directrices et règlements du CBP prévoient également des mesures disciplinaires sévères pouvant aboutir au licenciement à l'encontre de tout membre du personnel du CBP qui divulguerait des informations contenues dans les systèmes informatiques du CBP sans autorisation officielle (titre 19, section 103.34, du code des règlements fédéraux).

23) Est passible de sanctions pénales, y compris des amendes, un emprisonnement allant jusqu'à un an, voire les deux, tout fonctionnaire ou agent des États-Unis qui divulguerait des données de PNR obtenues dans l'exercice de ses fonctions lorsqu'une telle divulgation est interdite par la loi (titre 18, sections 641, 1030 et 1905 du code des États-Unis).

---

[6] Parmi les utilisateurs habilités du CBP figurent des agents affectés à des unités analytiques dans les bureaux locaux, ainsi que des agents affectés au Centre de ciblage national (*National Targeting Center*). Comme indiqué précédemment, les personnes chargées de la maintenance, du développement ou de l'audit de la base de données du CBP auront également accès à ces données, mais uniquement pour ces opérations.

[7] Bien que le dossier PNR ne soit pas techniquement supprimé lorsqu'il est transféré vers le fichier des dossiers supprimés, il est stocké sous la forme de données brutes (qui ne sont pas immédiatement interrogeables et ne peuvent donc pas être exploitées pour des enquêtes «traditionnelles») et est uniquement accessible au personnel habilité du Bureau des affaires internes (*Office of Internal Affairs*) du CBP et, dans certains cas, du Bureau de l'inspecteur général (*Office of the Inspector General*) en relation avec les audits ainsi qu'au personnel responsable de la maintenance de la base de données au sein du Bureau des technologies de l'information (*Office of Information Technology*) du CBP, en cas de besoin.

[8] L'accès par les «sous-traitants» aux données de PNR contenues dans les systèmes informatiques du CBP serait limité aux personnes ayant signé un contrat avec celui-ci pour l'aide à la maintenance ou au développement de son système informatique.

Traitement et protection des données de PNR par le CBP

24) Le CBP considère les informations du PNR, quels que soient la nationalité ou le pays de résidence de la personne concernée, comme des données sensibles au regard de l'exécution des lois et confidentielles, à caractère personnel dans le cas du passager ou relevant du secret commercial dans le cas de la compagnie aérienne, et ne devrait donc pas rendre ces données publiques, sauf dans les cas prévus par la présente déclaration d'engagement ou en vertu d'obligations légales en ce sens.

25) La divulgation de données de PNR est, de manière générale, régie par la loi sur la liberté de l'information (*Freedom of Information Act*, titre 5, section 552, du code des États-Unis), qui autorise toute personne quelle que soit sa nationalité ou son pays de résidence à consulter les registres d'une agence fédérale des États-Unis, sauf si ces registres échappent en tout ou partie à la divulgation en vertu d'une dérogation prévue par ladite loi. Parmi les dérogations possibles, la loi sur la liberté de l'information autorise une agence à protéger un registre en tout ou partie de la divulgation s'il contient des informations confidentielles à caractère commercial, si la divulgation est de nature à constituer une atteinte clairement injustifiée à la vie privée ou si les informations concernées sont établies à des fins répressives, dans la mesure où l'on peut raisonnablement penser que leur divulgation constituerait une atteinte injustifiée à la vie privée [titre 5, section 552(b)(4), (6), (7)(C) du code des États-Unis].

26) Les règlements relatifs au CBP (titre 19, section 103.12, du code des règlements fédéraux), qui régissent le traitement des demandes d'informations (par exemple concernant des PNR) en application de la loi sur la liberté de l'information, disposent spécifiquement que, sous réserve de certaines exceptions limitées dans le cas de demandes émanant des personnes concernées, les exigences établies en matière de divulgation par cette loi ne sont pas applicables aux registres du CBP concernant les informations confidentielles à caractère commercial, les éléments touchant à la vie privée dont la divulgation constituerait une atteinte clairement injustifiée à la vie privée et les informations établies à des fins répressives, lorsque l'on pourrait raisonnablement penser que leur divulgation constituerait une atteinte injustifiée à la vie privée [9].

27) Dans le cadre de toute procédure administrative ou judiciaire découlant d'une demande, introduite en vertu de la loi sur la liberté de l'information, de données de PNR obtenues auprès de compagnies aériennes, le CBP soutiendra que les registres en question ne sont pas soumis à la divulgation prévue par cette loi.

Transmission de données de PNR à d'autres autorités gouvernementales

28) Exception faite des transmissions entre le CBP et la TSA en application du paragraphe 8, les services du ministère de la sécurité intérieure seront traités comme des «organismes tiers» astreints aux mêmes règles et conditions pour le partage de données de PNR que les autres autorités gouvernementales extérieures audit ministère.

29) Le CBP, à sa discrétion, ne transmettra de données de PNR à d'autres autorités gouvernementales de répression ou de lutte contre le terrorisme, qu'elles soient nationales ou étrangères, qu'au cas par cas, aux fins de prévenir ou de combattre les crimes visés au paragraphe 3. Les autorités avec lesquelles le CBP peut partager ces données sont ci-après dénommées «autorités désignées».

30) Le CBP exercera avec discernement son pouvoir d'appréciation concernant le transfert de données de PNR aux fins spécifiées. Il déterminera tout d'abord si la raison invoquée pour la divulgation des données de PNR à une autre autorité désignée est conforme aux finalités prévues (voir le point 29). Dans l'affirmative, le CBP vérifiera si l'autorité désignée en question est compétente pour prévenir toute violation d'une loi ou d'un règlement lié à ces finalités ou pour mener une enquête ou engager des poursuites à cet égard ou pour mettre en œuvre ou veiller à l'application d'une telle loi ou d'un tel règlement, pour le cas où le CBP disposerait d'un indice d'une violation effective ou potentielle de la loi. Le bien-fondé de la divulgation devra être examiné à la lumière de l'ensemble des circonstances exposées.

31) Afin de réguler la diffusion de données de PNR pouvant être transmises à d'autres autorités désignées, le CBP est considéré comme étant «propriétaire» des données et les autorités désignées sont soumises, en vertu des conditions expresses de diffusion, aux obligations suivantes: 1) employer les données de PNR uniquement aux fins prévues au point 29 ou au point 34, selon les circonstances; 2) veiller à l'élimination systématisée des données de PNR communiquées, dans le respect des procédures de conservation mises en œuvre par l'autorité désignée, et 3) obtenir l'autorisation expresse du CBP avant toute nouvelle diffusion. Le non-respect des conditions de transfert peut donner lieu à une enquête et à un rapport du haut responsable de la vie privée auprès du ministère de la sécurité intérieure, à la suite de quoi l'autorité désignée en cause peut se voir privée du droit à tout transfert ultérieur de données de PNR par le CBP.

[9] Le CBP devrait appliquer ces dérogations de manière uniforme, indépendamment de la nationalité ou du pays de résidence de la personne concernée par les données.

32) Toute divulgation de données de PNR par le CBP est effectuée sous réserve que l'agence destinataire traite les données en question comme des informations confidentielles à caractère commercial et sensibles au regard de l'exécution des lois ou comme des informations confidentielles à caractère personnel pour les passagers, au sens des points 25 et 26, qu'il convient de considérer comme échappant à la divulgation prévue par la loi sur la liberté de l'information (titre 5, section 552 du code des États-Unis). De plus, l'agence destinataire sera informée que toute divulgation ultérieure des informations concernées est interdite sans l'autorisation préalable expresse du CBP. Le CBP n'autorisera aucun transfert ultérieur de données de PNR à des fins autres que celles prévues aux points 29, 34 ou 35.

33) Les membres du personnel des autorités désignées qui divulguent des données de PNR sans autorisation appropriée s'exposent à des sanctions pénales (titre 18, sections 641, 1030 et 1905 du code des États-Unis).

34) Aucune disposition de la présente déclaration d'engagement ne peut empêcher l'utilisation ou la divulgation de données de PNR aux autorités gouvernementales compétentes lorsque cette divulgation est essentielle à la protection des intérêts vitaux de la personne concernée ou d'autres personnes, notamment dans le cas de risques sanitaires graves. Les divulgations effectuées dans ce contexte obéissent aux mêmes conditions que celles applicables aux transferts qui sont décrites aux points 31 et 32.

35) Aucune disposition de la présente déclaration d'engagement ne peut empêcher l'utilisation ou la divulgation de données de PNR dans le cadre d'une procédure pénale ou au titre d'autres exigences prévues par la loi. Le CBP informera la Commission de l'adoption, par les autorités américaines, de toute législation ayant une incidence sur le fond des présents engagements.

Information, accès aux données et voies de recours pour les personnes concernées par les PNR

36) Le CBP portera à la connaissance des passagers les exigences relatives aux PNR et tous les éléments liés à leur utilisation, par exemple par la publication sur le site internet du CBP ou dans des dépliants à l'intention des voyageurs, de renseignements à caractère général concernant l'autorité responsable de la collecte des données, la finalité de la collecte, la protection des informations, le partage des données, l'identité du fonctionnaire responsable, les procédures de recours et les points de contact où soumettre les questions ou problèmes éventuels.

37) Les demandes émanant des personnes concernées (aussi dénommées «demandeurs au premier chef») et visant à obtenir une copie des informations de PNR les concernant figurant dans les bases de données du CBP sont traitées conformément à la loi sur la liberté de l'information. De telles demandes peuvent être adressées par courrier à l'adresse suivante: Freedom of Information Act (FOIA) Request, US Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Les demandes peuvent aussi être déposées auprès du Disclosure Law Officer, US Customs and Border Protection, Headquarters, Washington, D.C. Pour de plus amples informations concernant les procédures d'introduction de demandes relevant de la loi sur la liberté de l'information, voir la section 103.5 du titre 19 du code des réglementations fédérales. Dans le cas de demandes émanant des personnes concernées elles-mêmes, le fait que le CBP considère normalement les données de PNR comme des informations confidentielles à caractère personnel dans le cas des passagers ou relevant du secret commercial dans le cas des compagnies aériennes ne sera pas invoqué par le CBP en vertu de la loi sur la liberté de l'information pour ne pas communiquer les données de PNR aux personnes concernées.

38) Dans certaines circonstances exceptionnelles, le CBP peut faire usage de la faculté qui lui est conférée par la loi sur la liberté de l'information de refuser ou de reporter la divulgation de la totalité ou, plus probablement, d'une partie du dossier PNR à un demandeur au premier chef, conformément au titre 5, section 552 (b), du code des États-Unis (par exemple si l'on peut raisonnablement penser que la divulgation au titre de la loi sur la liberté de l'information est de nature à entraver une action répressive ou si cette divulgation aurait pour effet de révéler au grand jour des techniques ou procédures propres aux enquêtes judiciaires, au risque probable de permettre le contournement de la loi). La loi sur la liberté de l'information prévoit que tout demandeur est habilité à contester, par un recours administratif ou judiciaire, la décision du CBP de ne pas communiquer certaines informations (voir le titre 5, section 552(a)(4)(B) du code des États-Unis et le titre 19, section 103.7-103.9, du code des règlements fédéraux).

39) Le CBP s'engage à rectifier ([10]) des données à la demande de passagers ou de membres d'équipage, de compagnies aériennes ou d'autorités chargées de la protection des données d'États membres de l'Union européenne dans la limite du mandat conféré par la personne concernée lorsque le CBP établit que de telles données figurent dans sa base de données et juge la modification justifiée et étayée par les renseignements nécessaires. Le CBP informera toute autorité désignée ayant reçu les données de PNR en question de toute rectification de celles-ci.

([10]) En ce qui concerne cette possibilité de rectification, le CBP entend préciser qu'il n'est pas en son pouvoir de modifier les données contenues dans les dossiers PNR dont l'accès leur est ouvert auprès des compagnies aériennes. En lieu et place, un dossier distinct, lié au dossier PNR, sera établi pour mentionner que les données ont été reconnues erronées et indiquer les corrections nécessaires. Plus précisément, le CBP consignera dans le dossier d'examen secondaire (*secondary examination record*) du passager une mention signalant que certaines données du PNR sont (peut-être) erronées.

40) Les demandes de rectification de données de PNR contenues dans la base de données du CBP et les plaintes de particuliers concernant le traitement par le CBP de leurs données de PNR sont à envoyer, soit directement, soit par l'intermédiaire de l'autorité chargée de la protection des données compétente dans la limite du mandat conféré par la personne concernée, à l'adresse suivante: Assistant Commissioner, Office of Field Operations, US Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

41) Lorsqu'une plainte ne peut être tranchée par le CBP, il convient de l'adresser, par écrit, au haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure (*Chief Privacy Officer*, Department of Homeland Security, Washington, D.C. 20528), qui examinera la situation et s'efforcera de résoudre le litige ([11]).

42) De plus, le Bureau de la protection de la vie privée du ministère de la sécurité intérieure examinera en urgence les plaintes qui lui seront adressées par les autorités chargées de la protection des données dans les États membres de l'Union européenne pour le compte d'un résident de l'Union européenne, dans la mesure où ce résident a autorisé ces autorités à agir pour son compte et estime que sa plainte en matière de protection des données concernant les PNR n'a pas été traitée à sa satisfaction par le CBP, conformément aux paragraphes 37 à 41, ou par le Bureau de la protection de la vie privée du ministère de la sécurité intérieure. Ledit bureau rendra compte de ses conclusions et de toute mesure à l'autorité ou aux autorités concernées. Le haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure mentionnera, dans son rapport au Congrès des États-Unis, des renseignements quant au nombre, à la teneur et à l'issue des plaintes relatives au traitement des données à caractère personnel telles que les PNR ([12]).

Respect des dispositions

43) Le CBP, conjointement avec le ministère de la sécurité intérieure, s'engage à effectuer, une fois par an ou davantage suivant accord des parties, une révision commune avec la Commission, assistée au besoin de représentants des autorités répressives européennes et/ou des autorités des États membres de l'Union européenne ([13]), concernant la mise en œuvre de la présente déclaration d'engagement afin de contribuer au bon fonctionnement des modalités détaillées dans ladite déclaration.

44) Le CBP adopte les règlements, les directives ou toute autre mesure intégrant les présentes dispositions afin de garantir le respect des engagements par les fonctionnaires, agents et sous-traitants du CBP. Comme il est mentionné plus haut, le non-respect, par des fonctionnaires, agents ou sous-traitants du CBP, des règles établies par ces documents peut exposer à des mesures disciplinaires sévères, voire à des sanctions pénales le cas échéant.

Réciprocité

45) Dans l'éventualité où serait mis en œuvre dans l'Union européenne un système d'identification des passagers des compagnies aériennes qui ferait obligation à celles-ci de donner aux autorités l'accès aux données de PNR des passagers dont le voyage en cours inclut un vol à destination ou au départ de l'Union européenne, le CBP s'engage à encourager, à titre de réciprocité, les compagnies aériennes établies aux États-Unis à coopérer.

Révision et durée de validité de la déclaration d'engagement

46) La présente déclaration d'engagement est applicable durant une période de trois ans et six mois à compter de la date d'entrée en vigueur d'un accord entre les États-Unis et la Communauté européenne autorisant le traitement de données de PNR par les compagnies aériennes pour les transmettre au CBP conformément à la directive. À l'expiration de la période de deux ans et six mois de mise en œuvre de la présente déclaration d'engagement, le CBP, conjointement avec le ministère de la sécurité intérieure, entamera des discussions avec la Commission dans le but d'étendre les engagements et toute disposition connexe éventuelle, dans des conditions acceptables pour les deux parties. Si aucun accord acceptable pour les deux parties ne peut être trouvé avant la date d'expiration de la présente déclaration d'engagement, celle-ci cessera d'être applicable.

([11]) Le haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure n'est rattaché à aucune direction du ministère de la sécurité intérieure. Sa mission consiste à veiller à ce que les informations à caractère personnel soient utilisées dans le respect des lois applicables en la matière (voir note 13). Les décisions rendues par le haut responsable de la protection de la vie privée sont contraignantes pour le ministère, qui ne peut les annuler pour des motifs politiques.

([12]) Conformément à la section 222 de la loi de 2002 sur la sécurité intérieure (*Homeland Security Act — Public Law*, 107-296, du 25 novembre 2002), le haut responsable de la protection de la vie privée auprès du ministère de la sécurité intérieure a pour mission de procéder à une évaluation de l'impact sur la protection de la vie privée que pourraient avoir les mesures proposées par le ministère en ce qui concerne la confidentialité des informations à caractère personnel, y compris le type d'informations recueillies et le nombre de personnes concernées. En outre, il doit, chaque année, soumettre au Congrès un rapport portant sur les activités du ministère ayant une incidence sur la protection de la vie privée. Par ailleurs, la section 222, paragraphe 5, de ladite loi fait expressément obligation au haut responsable de la protection de la vie privée d'instruire toute plainte en matière d'atteinte à la vie privée et d'en faire rapport au Congrès.

([13]) Chaque partie devra, au préalable, informer l'autre de la composition de sa délégation, qui pourra regrouper des responsables des autorités compétentes en matière de protection des données ou de la vie privée, des autorités douanières et d'autres autorités répressives ou en charge de la sécurité des frontières et/ou de la sécurité des transports aériens. Les autorités participantes seront tenues d'obtenir toutes les autorisations nécessaires et respecteront la confidentialité des délibérations et des documents qu'elles pourraient être amenées à consulter. Cette exigence de confidentialité ne fera cependant pas obstacle à ce que chaque partie rende compte comme il se doit des résultats de la révision commune aux autorités nationales compétentes, dont le Congrès des États-Unis et le Parlement européen. En aucun cas cependant les autorités participantes ne pourront divulguer des informations à caractère personnel, des informations non publiques tirées de documents auxquelles elles pourraient avoir accès, ni des renseignements opérationnels ou internes relatifs à une agence dont elles auraient connaissance dans le cadre de la révision commune. Les deux parties arrêteront d'un commun accord les modalités détaillées de la révision.

Absence de création de droits ou de précédent

47) La présente déclaration d'engagement ne crée ni ne confère aucun droit ni aucun avantage pour toute personne ou partie, qu'elle soit privée ou publique.

48) La présente déclaration d'engagement ne constitue aucun précédent pour toute discussion ultérieure avec la Commission, l'Union européenne, toute organisation apparentée ou tout État tiers concernant le transfert de données sous quelque forme que ce soit.

Le 11 mai 2004

ANNEXE «A»

Rubriques des PNR demandées par le CBP aux compagnies aériennes

1. Code repère du dossier PNR
2. Date de réservation
3. Date(s) prévue(s) du voyage
4. Nom
5. Autres noms figurant dans le PNR
6. Adresse
7. Modes de paiement
8. Adresse de facturation
9. Numéros de téléphone
10. Itinéraire complet pour le PNR spécifique
11. Informations «grands voyageurs» [uniquement miles parcourus et adresse(s)]
12. Agence de voyage
13. Agent de voyage
14. Informations du PNR sur le partage de codes
15. «Statut» du voyageur (*Travel status of passenger*)
16. PNR scindé/divisé
17. Adresse électronique
18. Informations sur l'établissement des billets
19. Observations générales
20 Numéro du billet
21. Numéro du siège occupé
22. Date d'émission du billet
23. Passager répertorié comme défaillant
24. Numéros d'étiquetage des bagages
25. Passager de dernière minute sans réservation
26. Données OSI
27. Données SSI/SSR
28. Informations sur la source
29. Historique des changements apportés au PNR
30. Nombre de voyageurs dans le PNR
31. Informations relatives au siège occupé
32. Allers simples
33. Informations APIS éventuellement recueillies
34. Données ATFQ