4 - 1432/2

BELGISCHE SENAAT

ZITTING 2009-2010

28 OKTOBER 2009

Wetsontwerp houdende instemming met de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), gedaan te Brussel op 23 juli 2007 en te Washington op 26 juli 2007

VERSLAG

NAMENS DE COMMISSIE VOOR DE BUITENLANDSE BETREKKINGEN EN VOOR DE LANDSVERDEDIGING UITGEBRACHT DOOR

DE HEER **FONTAINE**

SÉNAT DE BELGIQUE

SESSION DE 2009-2010

28 OCTOBRE 2009

Projet de loi portant assentiment à l'Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007

RAPPORT

FAIT AU NOM DE LA COMMISSION DES RELATIONS EXTÉRIEURES ET DE LA DÉFENSE

PAR

M. **FONTAINE**

Samenstelling van de commissie / Composition de la commission :

Voorzitter / Présidente : Marleen Temmerman.

	Leden / Membres :	**Plaatsvervangers / Suppléants :**
CD&V	Sabine de Bethune, Els Schelfhout, Elke Tindemans, Els Van Hoof.	Wouter Beke, Cindy Franssen, Nahima Lanjri, Pol Van Den Driessche, Tony Van Parys.
MR	Alain Destexhe, Philippe Fontaine, Philippe Monfils.	Alain Courtois, Marie-Hélène Crombé-Berton, Christine Defraigne, Caroline Persoons.
Open VLD	Bart Tommelein, Paul Wille.	Nele Lijnen, Martine Taelman, Marc Verwilghen.
Vlaams Belang	Jurgen Ceder, Karim Van Overmeire.	Anke Van dermeersch, Freddy Van Gaever, Joris Van Hauthem.
PS	Philippe Mahoux, Olga Zrihen.	Christophe Collignon, Caroline Désir, Christiane Vienne.
sp.a	Fatma Pehlivan, Marleen Temmerman.	John Crombez, Guy Swennen, Myriam Vanlerberghe.
CDH	Jean-Paul Procureur	Dimitri Fourny, Vanessa Matz.
Écolo	Benoit Hellings.	Zakia Khattabi, Cécile Thibaut.

Zie :

Stukken van de Senaat :

4-1432 - 2008/2009 :

Nr. 1 : Wetsontwerp.

Voir :

Documents du Sénat :

4-1432 - 2008/2009 :

N 1 : Projet de loi.

I. INLEIDING

De commissie heeft dit wetsontwerp besproken tijdens haar vergadering van 28 oktober 2009.

II. INLEIDENDE UITEENZETTING DOOR DE HEER YVES LETERME, MINISTER VAN BUITENLANDSE ZAKEN

Het voorliggende wetsontwerp beoogt de goedkeuring van de Overeenkomst die werd afgesloten tussen de Europese Unie en de Verenigde Staten van Amerika zodat het mogelijk wordt om passagiersgegevens van luchtvaartmaatschappijen te bezorgen aan het ministerie van Binnenlandse Veiligheid van Amerika.

Na de terroristische aanslagen van 11 september 2001 heeft het Amerikaanse Congres een reeks wetten aangenomen om de binnenlandse veiligheid te versterken tegenover terroristische dreiging, waaronder de Amerikaanse wet van 19 november 2001 met betrekking tot de veiligheid van de luchtvaart en het vervoer.

Op basis van deze wet eisen de Amerikaanse douanediensten dat luchtvaartmaatschappijen die passagiersvluchten van, naar en over de VS organiseren, de gegevens van hun passagiers bezorgen. Ingeval zij dit niet doen, riskeren zij een vliegverbod van, naar en over de VS.

De informatie die moet worden verstrekt, zijn die gegevens die de passagier bezorgt wanneer hij/zij zijn vliegtuigticket aankoopt en die worden verzameld in de databanken van de vliegtuigmaatschappijen.

De privacyrichtlijn 95/46/EG, in Belgisch recht omgezet door de wet van 11 december 1998, verbiedt evenwel dat de lidstaten van de Europese Unie gegevens van persoonlijke aard zouden overmaken aan landen die deze gegevens niet op adequate wijze beschermen.

In mei 2004 werd een eerste akkoord afgesloten tussen de VS en de Europese Commissie waarin werd erkend dat de Amerikaanse douanediensten op adequate wijze bescherming bieden aan persoonsgegevens, op basis van hun geldende beschermingsregels op gegevens. Het Europese Hof van Justitie heeft dit akkoord echter geannuleerd, oordelend dat de juridische basis niet passend was. Nadien werd een nieuw akkoord afgesloten; dit akkoord ligt nu ter instemming voor.

Dit akkoord, waarover intensief werd onderhandeld, geeft het best mogelijke evenwicht weer tussen :

I. INTRODUCTION

La commission a examiné le projet de loi qui fait l'objet du présent rapport au cours de sa réunion du 28 octobre 2009.

II. EXPOSÉ INTRODUCTIF DE M. YVES LETERME, MINISTRE DES AFFAIRES ÉTRANGÈRES

Le projet de loi à l'examen vise à ratifier l'accord conclu entre l'Union européenne et les États-Unis d'Amérique prévoyant que les données relatives aux passagers détenues par les transporteurs aériens puissent être transférées au ministère américain de la Sécurité intérieure.

Au lendemain des attentats terroristes du 11 septembre 2001, le Congrès américain a adopté une série de lois visant à renforcer la sécurité intérieure face à la menace terroriste, notamment la loi du 19 novembre 2001 relative à la sécurité de l'aviation et des transports.

En vertu de ladite loi, les services douaniers américains exigent que les compagnies aériennes qui organisent des transports de passagers au départ ou à destination des États-Unis ou survolant le territoire américain transfèrent les informations sur leurs passagers. Si elles ne le font pas, elles risquent de se voir imposer une interdiction de vol au départ ou à destination des États-Unis, doublée d'une interdiction de survoler le territoire américain.

Les informations à transférer sont celles que le passager fournit lorsqu'il achète un billet d'avion et qui sont rassemblées dans les banques de données des transporteurs aériens.

La directive 95/46/CE relative à la vie privée, transposée en droit belge par la loi du 11 décembre 1998, interdit cependant que des États membres de l'Union européenne exportent des données à caractère personnel vers des pays qui n'offrent pas un niveau de protection adéquat pour ces données.

En mai 2004, un premier accord a été conclu entre les États-Unis et la Commission européenne. Cet accord reconnaît que les services douaniers américains offrent un niveau de protection adéquat pour les données personnelles, sur la base des règles américaines applicables en matière de protection des données. Cet accord fut pourtant annulé par la Cour européenne de justice qui a estimé que la base juridique n'était pas appropriée. Un nouvel accord a ensuite été conclu, et c'est cet accord qui est à présent soumis à assentiment.

Cet accord, qui a fait l'objet d'intenses négociations, représente le meilleur équilibre possible entre :

1. de noodzaak voor de luchtvaartmaatschappijen om rechtszekerheid te hebben,

2. de wenselijkheid om de goede betrekkingen met de Verenigde Staten in stand te houden,

3. de bescherming van de persoonsgegevens.

De overeenkomst bestaat uit :

— een overeenkomst die door de Verenigde Staten en de Europese Unie ondertekend is,

— een brief van de Verenigde Staten met eenzijdige verbintenissen van de Amerikaanse douanediensten inzake de bescherming van de gegevens,

— een antwoord van de Europese Unie waarin staat dat de Amerikaanse douanediensten voldoende bescherming bieden.

Wat de rechtszekerheid betreft, herinnert de minister eraan dat de luchtvaartmaatschappijen die niet ingaan op de Amerikaanse eis om de PNR-gegevens over te dragen in de Verenigde Staten sancties opgelegd krijgen : ze kunnen onder andere een vliegverbod naar de Verenigde Staten opgelegd krijgen. Er moest dus dringend een overeenkomst met de Verenigde Staten worden gesloten, om de rechtzekerheid van de Europese luchtvaartmaatschappijen te waarborgen en hun concurrentiepositie veilig te stellen.

Op diplomatiek gebied was het voor de Europese Unie belangrijk om snel tot een bevredigende overeenkomst met haar Amerikaanse partner te komen, in een materie die de nationale veiligheid van de Verenigde Staten, maar ook de veiligheid van Europa behelst, aangezien de PNR-gegevens nuttig kunnen zijn bij het opsporen van terroristische dreigingen, zowel in Europa als in de Verenigde Staten of elders.

Ten slotte werd er in het bijzonder aandacht besteed aan de bescherming van de persoonsgegevens.

De Verenigde Staten verbinden zich ertoe de Amerikaanse Privacy Act, die tot dusver alleen voor de Amerikaanse burgers gold, uit te breiden tot de Europese burgers. Dat is een belangrijk aspect van dit dossier.

Op die manier worden de Europese burgers erover ingelicht dat de Amerikaanse douanediensten hun gegevens verwerken om het terrorisme te bestrijden en dat zij — de burgers — recht hebben op toegang tot hun gegevens, op rectificatie en op administratief beroep.

De gegevens worden 7 jaar actief bewaard en acht jaar in een slapende status.

Tegenover die verbintenissen staat dat de Europese Unie verklaart dat de Amerikaanse douanediensten voldoende bescherming bieden.

1. la nécessité pour les compagnies d'aviation d'avoir une sécurité juridique,

2. la nécessité de maintenir des bonnes relations avec les États-Unis,

3. la protection des données à caractère personnel.

L'accord est composé :

— d'un accord signé par les États-Unis et l'Union européenne,

— d'une lettre des États-Unis comportant des engagements unilatéraux des douanes américaines en matière de protection des données,

— d'une réponse de l'Union européenne considérant que les douanes américaines offrent un niveau de protection adéquat.

En ce qui concerne la sécurité juridique, le ministre rappelle que les transporteurs aériens qui ne satisfont pas à l'exigence américaine de transférer les données PNR encourent des sanctions aux États-Unis : ils peuvent notamment se voir imposer une interdiction de vol à destination des États-Unis. Il était donc impératif et urgent de conclure un accord avec les États-Unis afin de garantir la sécurité juridique des compagnies aériennes européennes et de préserver leur situation concurrentielle.

Sur le plan diplomatique, il était important pour l'Union européenne de trouver rapidement un accord satisfaisant avec son partenaire américain, dans une matière touchant à la sécurité nationale des États-Unis mais également à la sécurité européenne puisque les données PNR peuvent contribuer à détecter des menaces terroristes tant en Europe qu'aux États-Unis ou ailleurs.

Enfin, une attention particulière a été prêtée à l'aspect protection des données personnelles.

Les États-Unis s'engagent à étendre aux citoyens européens le Privacy act américain, applicable jusqu'alors aux seuls citoyens américains. Il s'agit d'un aspect important dans ce dossier.

De la sorte, les citoyens européens sont informés que les douanes américaines traitent leur données à des fins de lutte contre le terrorisme, et ont un droit d'accès à leurs données, de rectification et de recours administratif.

Les données sont conservées durant 7 ans de manière active et huit ans de manière dormante.

En échange de ces engagements, l'Union européenne déclare que les douanes américaines offrent un niveau de protection adéquat.

Deze Overeenkomst, gesloten in samenspraak met onze Europese partners, biedt het best mogelijke evenwicht tussen de verschillende bezorgdheden en biedt tevens alle gewenste garanties inzake bescherming van de privacy van onze burgers.

III. GEDACHTEWISSELING

Mevrouw Zrihen wijst erop dat de maatregelen die de Amerikaanse luchtvaartmaatschappijen hebben genomen veel verder gaan dan die welke andere maatschappijen hebben genomen van landen die soortgelijke spanningen en terrorismedreigingen kennen. De persoonsgegevens dienen om de toegang tot het grondgebied te verbieden. De tekst van de Overeenkomst maakt het onmogelijk de regeling terug te draaien. De Commissie voor de Bescherming van de Persoonlijke Levenssfeer had voorbehoud gemaakt inzake dit voorstel, omdat ze het niet zo evenwichtig vond als men mag verwachten op het vlak van de eerbiediging van de burgers en van de gegevens in verband met hun privéleven.

De luchtvaartmaatschappijen worden zeer zwaar onder druk gezet. Indien ze een aantal gegevens niet bezorgen, dreigen ze te worden bestraft. Het is niettemin noodzakelijk een lijst te maken van punten die in elk geval specifiek moeten worden bekeken bij een evaluatieproces. In 2001 was er evenmin sprake van de Verenigde Staten automatisch een vrijbrief te geven voor dergelijke zaken. Hem in de huidige omstandigheden blijven geven, zou buiten alle proporties zijn.

De heer Fontaine meent dat de Europese landen misschien niet dezelfde gevoeligheden hebben als de Verenigde Staten van Amerika inzake veiligheid en personencontrole. De gegevens kunnen in de Verenigde Staten misbruikt worden. Hoe kan men nagaan of de vertrouwelijkheid van de persoonsgegevens in acht werd genomen ?

De heer Hellings wenst te weten op grond waarvan precies de gegevens in deze context worden bewaard.

Mevrouw de Bethune is van oordeel dat het bestaan van een verdragsrechtelijke basis in deze materie rechtszekerheid biedt. Er moet wel worden nagegaan of er voldoende garanties bestaan voor de bescherming van de persoonlijke levenssfeer. Spreekster verwijst naar het advies van de Raad van State waarin gesteld wordt dat :

« De groep gegevensbescherming artikel 29 heeft op 17 augustus 2007 zijn goedkeuring gehecht aan advies 5/2007 over de follow-upovereenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door lucht-

Cet accord, conclu en concertation avec nos partenaires européens, offre le meilleur équilibre possible entre les différentes préoccupations ainsi que toutes les garanties souhaitées en matière de protection de la vie privée de nos citoyens.

III. ÉCHANGE DE VUES

Mme Zrihen signale que les mesures prises par les compagnies ariennes américaines dépassent largement celles prises par les autres compagnies des pays qui pourraient vivre des tensions et menaces similaires de terrorisme. Les données relatives à la vie privée servent à interdire l'accès au territoire. Le dispositif prévu par l'Accord ne permet pas de revenir en arrière. La Commission pour la Protection de la Vie privée était réticente à cette proposition, ne trouvant pas l'équilibre qu'on est en droit d'attendre par rapport au respect dû aux citoyens et aux données qui concernent leur vie privée.

La pression mise sur les transporteurs est très forte. S'ils ne transmettent pas un certain nombre d'informations, ils risquent de se trouver pénalisés. Il y a quand même nécessité d'établir une liste d'éléments qui doit absolument faire l'objet d'un suivi spécifique dans le cadre d'un processus de réexamen. Déjà en 2001, il n'a pas été question de donner un blanc seing automatique aux États-Unis en ce qui concerne ce type de démarche. Il serait excessif de continuer à le donner dans les conditions actuelles.

M. Fontaine estime que les pays européens n'ont pas nécessairement les mêmes sensibilités que les États-Unis d'Amérique en matière de sécurité et de contrôle des personnes. Des abus peuvent se produire au niveau des États-Unis. Comment peut-on vérifier si la confidentialité des données privées est respectée ?

M. Hellings souhaite savoir sur la base de quels critères précis, les données sont conservées dans ce cadre.

Mme de Bethune estime que l'existence d'une base conventionnelle offre une sécurité juridique en la matière. Il faut en revanche contrôler s'il y a suffisamment de garanties pour la protection de la vie privée. L'intervenante renvoie à l'avis du Conseil d'État qui affirme que :

« Le groupe de travail « Article 29 » sur la protection des données a adopté le 17 août 2007 l'avis 5/2007 concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens

vaartmaatschappijen aan het ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika, gesloten in juli 2007

Dat advies zou als een bijlage moeten worden gevoegd bij het voorontwerp van wet houdende instemming met de overeenkomst, aangezien dat advies dit voorontwerp in perspectief plaatst en een nuttige aanvulling vormt van de memorie van toelichting en dit advies.

Om dezelfde redenen zou ook het advies van 25 oktober 2007 van de Juridische Dienst van het Europees Parlement betreffende de Overeenkomst als bijlage bij het parlementair stuk gevoegd moeten worden. » (stuk, nr. 4-1432/1, blz. 38)

Het advies van 25 oktober van de Juridische Dienst van het Europees Parlement zou vertrouwelijk zijn. Mag dit gepubliceerd worden ?

De heer Mahoux wenst te weten wie op het niveau van de Europese Unie over de Overeenkomst onderhandeld heeft. De PNR-gegevens bestrijken een zeer breed veld en hebben met heel delicate aspecten van de privacy te maken. Hoe lang worden die gegevens overigens bewaard en is die periode overeenkomstig het Belgisch recht ? Hoewel men het vliegtuig vrijwillig neemt, moet men worden beschermd tegen misbruik van persoonsgegevens.

Mevrouw de Bethune merkt op dat er reeds verschillende landen van de Europese Unie deze overeenkomst geratificeerd hebben. Op welke wijze werd in deze landen de Overeenkomst toegepast ?

Mevrouw Temmerman wenst te weten welke landen deze Overeenkomst hebben geratificeerd.

Verder vestigt mevrouw Temmerman de aandacht op de gevoeligheid van de informatie en verwijst zij naar de vragen die recent in het openbaar aan een Afrikaanse collega werden gesteld in verband met AIDS/HIV.

ANTWOORDEN VAN DE MINISTER VAN BUITENLANDSE ZAKEN

De minister legt uit dat er een limitatieve lijst is opgesteld van de persoonsgegevens betreffende passagiers (PNR gegevens) die worden ingezameld. Het zijn alleen die gegevens die onder het toepassingsbied van de Overeenkomst vallen en die dus het voorwerp uitmaken van bewaring. Tickets hebben een code waardoor informatie kan worden behouden. Verder zijn er ook, onder andere, de datum van reservering en uitgifte van het ticket, de datum van de reis, de naam van de houder en het aantal gratis tickets, de PNR-gegevens, evenals het overzicht van het ticketgebruik. De contactgegevens, de reisroute, het reisagentschap en de bagage worden eveneens als PNR-gegevens

au ministère américain de la sécurité intérieure (DHS), conclu en juillet 2007.

Cet avis mériterait d'être annexé à l'avant-projet de loi portant assentiment à l'accord, car il met celui-ci en perspective et constitue un complément utile à l'exposé des motifs et au présent avis.

Pour les mêmes raisons, l'avis du 25 octobre 2007 du service juridique du Parlement européen relatif à l'Accord mériterait lui aussi d'être joint au document parlementaire. » (doc. Sénat, n° 4-1432/1, p. 38)

L'avis du 25 octobre 2007 du service juridique du Parlement européen serait confidentiel. Peut-il être publié ?

M. Mahoux souhaite savoir qui a négocié l'Accord au niveau de l'Union européenne. Les données PNR recouvrent un champ très étendu et touchent à des aspects très sensibles de la vie privée. Quel est par ailleurs la durée de conservation de ces données et est-elle conforme au droit belge ? Bien qu'on prenne l'avion de manière volontaire, il faut être protégé contre des abus d'utilisation de données de la vie privée.

Mme de Bethune signale que plusieurs États membres de l'Union européenne ont déjà ratifié cet accord. Comment l'ont-ils appliqué ?

Mme Temmerman aimerait savoir de quels pays il s'agit.

Elle met ensuite l'accent sur le caractère sensible des informations et renvoie aux questions qui ont récemment été posées en public à un collègue africain au sujet du sida/VIH.

RÉPONSES DU MINISTRE DES AFFAIRES ÉTRANGÈRES

Le ministre explique que les données des dossiers passagers (données PNR) collectées ont été définies dans une liste limitative. Ce sont les seules données qui relèvent du champ d'application de l'accord et qui sont donc conservées. Les billets d'avion sont dotés d'un code, ce qui permet de répertorier les informations. Parmi les données PNR, il y a aussi, entre autres, la date de réservation et d'émission du billet, la date du voyage, le nom du titulaire, le nombre de billets gratuits ainsi que l'historique de l'utilisation du billet. Les informations de contact, les informations relatives à l'itinéraire, à l'agence de voyage et aux bagages, les informations « PNR scindé », les informations OSI et

beschouwd, alsook de informatie betreffende de gesplitste PNR- en de OSI- en SSI/SSR-gegevens en de API-gegevens die voorkomen op het ticket (zie punt III van de overeenkomst, betreffende de soorten verzamelde informatie, stuk Senaat, nr. 4-1432/1, p. 29-30).

De OSI gegevens en SSI/SSR gegevens zijn optioneel en hebben betrekking op de vraag naar specifieke diensten, zoals gehandicaptenbegeleiding of voedselkeuze.

Die gegevens worden eruit gefilterd voor ze door het Department of Homeland Security (DHS) worden ingezameld. Indien sleutelwoorden opduiken, zoals geneeskundig of halal, blokkeert de filter die gegevens. De filter wordt regelmatig opnieuw bekeken bij de gezamenlijke evaluatie door de Europese Unie en de DHS. De eerste gezamenlijke evaluatie vindt pas in maart 2010 plaats, omdat men nog niet weet of de Data Protection Officer terzake bevoegd zal zijn.

Wat betreft de ongeoorloofde verspreiding van PNR- gegevens, voorziet de Amerikaanse Privacy Act een aantal administratieve, burgerechtelijke en strafrechtelijke sancties.

De DHS staat de toegang tot de PNR-gegevens aan de desbetreffende personen toe, ook aan de onderdanen van de Europese Unie, om informatie over die gegevens te krijgen of om ze te corrigeren.

Het gaat om het zelfde type toegang zoals bepaald door richtlijn 95/46/EG van de Europese Unie.

Er wordt over de Overeenkomst onderhandeld door het Commissielid voor de Justitie van de Commissie van de Europese Unie en door het voorzitterschap van de Unie. Tevens werd de principiële beslissing om over de eerste Overeenkomst te onderhandelen in 2001 genomen, tijdens het Belgisch voorzitterschap van de Europese Unie.

Document nr. SJ-0634/07 van 25 oktober 2007 van het Europees Parlement betreffende de bescherming van personen tegen de overdracht van privégegevens in de Overeenkomst wordt bij dit verslag gevoegd.

IV. STEMMINGEN

De artikelen 1 en 2 worden aangenomen met 8 stemmen bij 1 onthouding. Het wetsontwerp in zijn geheel wordt aangenomen met 7 stemmen bij 2 onthoudingen.

*
* *

SSI/SSR ainsi que les informations APIS figurant sur le billet sont également considérées comme des données PNR (voir le point III de l'accord qui porte sur les types de données PNR collectées, doc. Sénat, n° 4-1432/1, pp. 29-30).

Les données OSI et SSI/SSR sont optionnelles et ont trait à la demande de services spécifiques comme l'accompagnement de personnes handicapées ou le choix des repas.

Ces données sont filtrées même avant leur collecte par le *Department of Homeland Security* (DHS). Si des mots-clefs apparaissent, tels que médical ou halal, le filtre bloque les données. Ce filtre est régulièrement revu lors du réexamen conjoint entre l'Union européenne le DHS. Le premier réexamen conjoint n'a lieu qu'en mars 2010 parce que on ne sait pas encore si le Data Protection Officer sera compétent en la matière.

En ce qui concerne la divulgation non autorisée de données PNR, la loi américaine sur le respect de la vie privée (Privacy Act) prévoit un certain nombre de sanctions administratives, civiles et pénales.

Le DHR permet l'accès aux données PNR aux personnes concernées, y compris les ressortissants de l'Union européenne, pour des renseignements sur ces données ou la correction de celles-ci.

Il s'agit du même type d'accès que celui prévu par la directive 95/46/CE de l'Union européenne.

La négociation de l'Accord se fait par le Commissaire pour la Justice auprès de la Commission de l'Union européenne ainsi que par la présidence de l'Union. Par ailleurs, la décision de principe de négocier le premier accord a été prise en 2001 lors de la présidence belge de l'Union européenne.

Le document n° SJ-0634/07 du Parlement européen du 25 octobre 2007 sur la protection des personnes contre le transfert de données privées au sein de l'Accord est annexé au présent rapport.

IV. VOTES

Les articles 1er et 2 sont adoptés par 8 voix et 1 abstention. L'ensemble du projet de loi est adopté par 7 voix et 2 abstentions.

*
* *

Vertrouwen wordt geschonken aan de rapporteur voor het opstellen van dit verslag.

De rapporteur, *De voorzitter,*

Philippe FONTAINE. Marleen TEMMERMAN.

*
* *

De door de commissie aangenomen tekst is dezelfde als de tekst van het wetsontwerp (stuk Senaat, nr. 4-1432/1 - 2008/2009).

*
* *

Confiance a été faite au rapporteur pour la rédaction du présent rapport.

Le rapporteur, *La présidente,*

Philippe FONTAINE. Marleen TEMMERMAN.

*
* *

Le texte adopté par la commission est identique au texte du projet de loi (doc. Sénat, n° 4-1432/1 - 2008/2009).

*
* *

BIJLAGE | **ANNEXE**

European Parliament

Legal Service

SJ-0634/07

KB/AC/hr

Strasbourg,

D(2007)65222

LEGAL OPINION

This document is a confidential legal opinion within the meaning of Article 4 (2) of Regulation 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. The European Parliament reserves all its rights should this be disclosed without its authorisation.

Re : 2007 Passenger Name Record (PNR) Agreement between EU and U.S. — Council Decision — General principles and fundamental rights — Protection of individuals with regard to the processing and transfer of personal data

I. INTRODUCTION

By letter dated 10 September 2007 (annex), Mr Jean-Marie CAVADA, chairman of the Committee on Civil Liberties, Justice and Home Affairs (hereinafter, « LIBE »), requested a legal opinion on the new Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (hereinafter, « PNR ») data by air carriers to the United States Department of Homeland Security (hereinafter, « DHS ») signed in Brussels and in Washington on 23 and 26 July 2007 (hereinafter, « 2007 PNR Agreement ») (1).

Mr CAVADA raised a number of issues concerning the Agreement and also referred to paragraph 31 of Parliament's Resolution of 12 July 2007 stating its intention « to seek a legal appraisal of the new PNR Agreement for conformity with national and EU legislation » (2).

II. THE 2007 PNR AGREEMENT

On 30 May 2006, the European Court of Justice annulled (3) the Council Decision on the conclusion of the first PNR Agreement between the European Community and the United States of America and the Commission Decision which recognised, on the basis of Article 25 of Directive 95/46/EC, the U.S. as providing an adequate level of protection for the transfer of PNR data (4). The Court held that PNR data processing at issue was outside the scope of Directive 95/46/EC (5).

A new interim PNR Agreement (6) was concluded on 19 October 2006 on the basis of Articles 24 and 38 of the EU Treaty (7). This Agreement, as provided for in its Article 7, expired on 31 July 2007.

(1) OJ L 204 of 4 August 2007, p. 18. See also the Council Decision 2007/551/CFSP/JHA of 23 July 2007 (hereinafter, « the Council Decision ») on the signing, on behalf of the European Union, of this Agreement, OJ L 204 of 4 August 2007, p. 16.

(2) P6 TA-PROV(2007)0347.

(3) Judgment of 30 May 2006 in Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission, the « PNR » case [2006] ECR I-4721.

(4) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, page 31.

(5) The Court of Justice held that « the transfer of PNR data to CBP [U.S. Bureau of Custom and Border Protection] constitutes processing operations concerning public security and the activities of the State in areas of criminal law' » (paragraph 56).

(6) OJ L 298 of 27 October 2006, p. 29. See also the Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union of this Agreement, OJ L 298 of 27 October 2006, p. 27.

(7) Article 38 EU provides that agreements referred to in Article 24 may cover matters falling under the Title VI of the EU Treaty. This means that the procedure provided for in Article 24 EU applies.

The 2007 PNR Agreement (1) is also based on Articles 24 and 38 EU. These provisions expressly recognise the competence of the Council to conclude such agreements (2), but do not provide for any direct participation of the European Parliament in their negotiation or conclusion (3). according to Article 24(6) EU, such Agreements « shall be binding on the institutions of the Union ».

In accordance with the first recital in the preamble and Clause 1 (4) of this Agreement, the European Union undertakes to « ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America will make available PNR data contained in their reservation systems as required by DHS » in order to prevent and combat terrorism and transnational crime effectively as a means of protecting EU and U.S. democratic societies and common values.

7. The 2007 PNR Agreement contains a set of assurances given by the DHS in the U.S. letter to EU (hereinafter, « the U.S. letter ») annexed to the Agreement. Clause 1 indicates that the transfer of PNR data is authorised on the basis of the assurances given by the DHS. Clause 6 provides that for its application, « DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union » and that concomitantly, « the EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds ».

8. In the EU letter to US. (hereinafter, « the EU letter »), the President of the Council, Mr Luis AMADO states that the assurances provided in the U.S. letter « allow the European Union to deem, for the purpose of the international agreement signed between the United States and European Union on the processing and transfer of PNR in July 2007, that DHS ensures an adequate level of data protection ».

9. Clause 9 of the 2007 PNR Agreement provides that the Agreement will be applied provisionally as of the date of the signature (26 July 2007) and Recital 6 of the Council Decision authorising the signature of the Agreement states that « Member States should therefore give effect to its provisions as from that date in conformity with existing domestic law ».

III. THE LEGAL FRAMEWORK

10. While both Mr Cavada's letter and European Parliament's Resolution of 12 July 2007 require a legal evaluation of the 2007 PNR Agreement, it should be noted at the outset that neither the EU Treaty nor any applicable EU or EC legislation provides specific criteria against which to judge the validity of this Agreement. In particular, Directive 95/46/EC does not apply in these circumstances (5), and the proposed Council Framework Decision on data protection in the context of police and judicial cooperation in criminal matters (Title VI of the EU Treaty) has not been adopted (6). The protections provided under the 1995 Directive do not apply in Title VI of the EU Treaty, and there is no equivalent procedure for recognising the adequate level of personal data protection in third countries.

11. It should be noted nonetheless that the 2007 PNR Agreement, in the seventh recital in the preamble, refers to Article 6(2) EU, which recognises explicitly the European Union's duty to respect fundamental rights « as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950, and as they result from the constitutional traditions common to the Member States, as general principles of Community law ». The same recital refers « in particular to the related right to the protection of personal data ». The fact that the Agreement refers to these different rights indicates that the Council intended to respect them and hence they should be considered relevant in evaluating the validity of the Agreement.

(1) On 22 February 2007 the Council decided to authorise the Presidency, assisted by the European Commission, to open negotiations with the U.S. authorities for a long-term agreement on PNR. The result of those negotiations is the 2007 PNR Agreement.

(2) Article 24(1) EU provides that « the Council may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations [... to the effect to conclude agreements]. Such agreements shall be concluded by the Council on a recommendation fro the Presidency ».

(3) However, Article 21 EU provides that the « Presidency shall consult the European Parliament on the main aspect and the basic choices of the common foreign and security policy and shall ensure that the views of the European Parliament are duly taken into consideration. The European Parliament shall be kept regularly informed by the Presidency and the Commission of the development of the Union's foreign and security policy ».

(4) For convenience, the numbered provisions of the Agreement are referred to as « Clauses », and those of the U.S. letter as « Paragraphs ».

(5) The legal context of Titles V and VI of the EU Treaty is substantially different from that of the EC Treaty. See the « PNR » judgment cited above, paragraph 54.

(6) 2005/0202(CNS) — COM(2005) 475 final of 4 October 2005 [SEC(2005) 1241].

A. The European Convention on Human Rights

12. Article 8 of the European Convention for the protection of Human Rights (ECHR) provides for the respect for private life (1). The right to privacy is not an absolute one and it must therefore be balanced with other interests, such as law enforcement (2). Member States can take privacy or personal data-intrusive measures upon condition that these are necessary for the enforcement of criminal law. Article 8(2) of the ECHR clearly specifies that there shall be no interference by a public authority with the exercise of the right of privacy (including the protection of personal data) unless the interference is in conformity with the law and is necessary in a democratic society for the protection of public order and the prevention of crime. Member States have a certain margin of appreciation in adopting and implementing internal rules in accordance with the principles of the ECHR.

13. The mere storing of personal data, irrespective its possible future use, must be considered, in the light of the ECHR Court's case law, as an interference with the right to privacy. In its judgment of 16 February 2000, in Amann v Switzerland, the European Court of Human Rights stated that « the storing by a public authority of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding » (3).

14. In addition, any restriction on the right to privacy and to protection of personal data must be based on law. The ECHR Court refers to one formal requirement, that is to say the existence of a domestic law, and to one substantive requirement, that is to say the quality of the law in dispute, which has to be compatible with the rule of law (4). There are also the requirements of accessibility and foreseeability of the law (5).

15. In its judgment Amann v Switzerland, the European Court of Human Rights stated an interference « in accordance with the law not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects » (6). In Copland v United Kingdom, the Court held that « in order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to circumstances in which and the conditions on which the authorities are empowered to resort to any such measures » (7).

16. The European Court of Human Rights also requires that any interference justified in accordance with Article 8(2) ECHR respect the principle of proportionality. In the present case, the question is whether the treatment and transfer of PNR data governed by the 2007 PNR Agreement exceed what is necessary to achieve to objective of fighting terrorism and other serious international crimes as provided for in the text of the Agreement, and whether or not there was any manifest error of assessment on the part of the EU Council.

17. Personal data is also protected in accordance with Article 8 of the Charter of Fundamental Rights of the European Union (8). Paragraph 2 of this Article provides that « such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified » (9).

B. Council of Europe Convention 108

18. All the Member States are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981 (Convention 108). The principles it establishes may be considered as the most authoritative statements of general principles governing the protection of personal data (10).

---

(1) The case-law of the ECHR Court is taken into account by the Court of Justice for the interpretation of the provisions of the ECHR (see judgments of 6 March 2001, in Case C-274/99 P, Connolly, [2001] ECR I-1611, and of 11 July 2002, in Case C-60/00, Carpenter, [2002] ECR I-6279).

(2) See also the third to fifth paragraphs of page 6 of Opinion 5/2007 of the Article 29 Data Protection Working Party (17 August 2007, 01646/07/EN, WP 138).

(3) Paragraph 69 of the ECHR Court's judgment.

(4) Judgment of 2 August 1984, in Malone v United Kingdom, paragraph 87.

(5) Judgment of 26 April 1979, in Sunday Times v United Kingdom, paragraph 49.

(6) Paragraph 50 of the ECHR Court's judgment.

(7) Paragraph 46 of the ECHR Court's judgment

(8) OJ C 364 of 18 December 2000, p. 1.

(9) Even if the Charter does not have a binding character, the Court of Justice has recently cited the Charter and has acknowledged its importance. See paragraphs 38 and 58 of the Court's judgment of 27 June 2006, in Case C-540/03, European Parliament v Council, Right to family reunification [2006] ECR I-5769.

(10) The principles set down in Convention 108 are not dissimilar from those included in OECD (Organisation for Economic Co-operation and Development) Privacy Guidelines of 1980 and in the United Nations Guidelines of 1990.

19. The purpose of Convention 108, as provided for in Article 1, is « to secure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedom, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ». according to Article 4(1) of Convention 108, each State Party « shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out » in the Convention.

20. Article 5 of the Convention 108 requires that data processed automatically shall be :

« (a) obtained and processed fairly and lawfully;

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, where necessary, kept up to date;

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

21. To these basic criteria Article 6 adds safeguards concerning special categories of data :

« personal data revealing racial origin, political opnions or religious or other beliefs, as well as personal data concerning health and sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions ».

22. Other criteria normally taken into consideration are the right of access to personal data for the person concerned and the right of redress. Article 7 provides that « appropriate security measures shall be taken for the protection of personal data stored in automatic data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination ».

23. Article 8 of Convention 108 provides that any person shall be enabled :

« a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraph b and c of this Article is not complied with ».

24. According to Article 9(2) :

« derogation from the provisions of Article 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of :

a. protection State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others ».

25. Drawing inspiration from both Directive 95/46/EC and the 2001 Additional Protocol to Convention 108 (1), the Member States have decided to adopt a common approach to determining whether a particular third State guarantees an adequate level of data protection because of the European Union competencies in Titles V and VI of the EU Treaty. The 2007 PNR Agreement therefore seeks to establish the conditions for recognising that the U.S. ensures an adequate level of protection (2).

(1) Additional Protocol 181 to Convention 108 seeks in effect to ensure the Convention protections are respected in international exchanges of personal data. Article 2 (1) provides that each Party to the Convention « shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensure an adequate level of protection for the intended data transfer11 (emphasis added). While not all Member States are parties to the Protocol, it appears from the text of the Agreement that the Council sought to respect this provision as part of the general principles governing the transfer of personal data.

(2) National laws and rules of those States which have ratified the Additional Protocol must be consistent with the above provisions. In the light of these provisions, there is a clear obligation for Member States which are Parties to the Convention to verify whether the level of protection of a third country is adequate.

IV. LEGAL ANALYSIS

IV.A. Does the 2007 PNR Agreement respect European Union data protection principles ?

26. While the compatibility of the PNR Agreement with data protection principles raises a large number of complex legal issues, it is proposed only to examine the following matters in the present opinion : purpose limitation, type and number of data required, duration of data retention, access to information and redress, and dissemination of PNR data.

27. In analysing the 2007 PNR Agreement, it has to be recalled that every treaty is binding upon the Parties to it and must be performed by them in good faith (1).

(a) Purposes for which PNR data are required

28. From the preamble, it appears that the Agreement is designed « to prevent and combat terrorism and transnational crime11 in which context « PNR data is an important tool ». The limitation of the use of PNR data to the prevention and combating of terrorist and other serious transnational crimes is repeated in the first sentence of Paragraph I of the U.S. letter which reads as follows :

« DHS uses EU PNR strictly for the purpose of preventing and combating : (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are international in nature; and (3) flight from warrant or custody for crimes described above ».

29. However, the second sentence of Paragraph I goes on to specify that « PNR may be used where necessary for the protection of the vital interest of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law ».

30. At best, the wording of this provision is ambiguous. On one interpretation, the restrictions set out in the two sentences could be deemed cumulative. Under this view, PNR could only be used for preventing the three types of activity listed in the first sentence, and within this context it may be used in the three sets of circumstances indicated in the second sentence, that is, protecting the data subject, in criminal proceedings and as otherwise required by law.

31. This interpretation is probably not, however, that intended by the U.S. letter. Paragraphs 34 and 35 of the Undertakings provided by the DHS at the time of the conclusion of the 2004 PNR Agreement (2) allowed the disclosure of PNR data to other government agencies in these three circumstances, albeit only on a case-by-case basis. The new text would appear to allow systematic disclosure of such data, as well as their transfer to foreign governments and to other U.S. government agencies.

32. If the restrictions in the first and second sentences of Paragraph I of the U.S. letter were to be interpreted as alternatives, it would mean that the purposes for PNR data could be used would be extremely wide indeed, including « where necessary [...] in any criminal judicial proceedings, or as otherwise required by law. » The restrictions of the first sentence would to a large extent be inoperative.

33. The fact that the two sentences are differently worded would also support the view that they are intended to be alternatives. The first sentence appears to describe the current state of affairs (« DHS uses »), while the second appears to refer to the future (« PNR may be used »).

34. In addition, the wording of the second sentence seems to refer to specific cases (« protection of the vital interest of the data subject or other persons »); this literal interpretation would indicate that the two restrictions govern distinct situations.

35. The consequence is that, under its most natural interpretation in the circumstances, the DHS letter refers to data processing for general rather than specified purposes, contrary to one of the principal criteria governing the processing of personal data.

(b) Type and number of personal data

36. The criteria for evaluating the adequate level of protection given by DHS are contained in Convention 108 and, more specifically, in its Articles 5 and 6. It is important to point out that « adequate » does not imply an equal or similar level of data protection.

(3) See Article 26 (Pacta sunt servanda principle) and Article 31(1) on the general rule of interpretation of the 1969 Vienna Convention on the Law of Treaties.

(2) Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), OJ L 235 of 6 July 2004, p. 15.

37. The 19 types of PNR data listed in Paragraph III of the U.S. letter can be considered as appropriate information necessary for combating terrorism and other serious crime. The data requested are *prima facie* related to the profiling of persons who could be involved in the preparation or realisation of terrorist attacks. As has been pointed out by Advocate General Léger in the PNR Case « the importance of intelligence activity in counter-terrorism should be stressed, since obtaining sufficient information may enable a State's security services to prevent a possible terrorist attack. From that point of view, the need to profile potential terrorists may require access to a large number of pieces of data ». The Advocate General went on to opine that « the fact that other instruments relating to the exchange of information adopted within the European Union provide for disclosure of less data is not sufficient to demonstrate that the amount of data required ... by the PNR regime is excessive » (1).

38. The importance of the fight against terrorism in the action of the European Union is demonstrated by the number of and scope of the measures adopted to date. These include not only the Council Framework Decision 2002/475/JHA on combating terrorism and similar measures (2), but also a comprehensive couter-terrorism strategy (3). The prevention of this criminal phenomenon requires specific measures for profiling and finding persons who may be involved in terrorism-related activities.

39. Therefore, there is no evidence that the amount of data required in the PNR regime, which may be considered a specific counter-terrorism instrument, is necessarily excessive and unjustified.

40. It is nonetheless surprising that some sensitive data, such as personal data revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, etc., can be collected by the air carriers. according to the penultimate subparagraph of Paragraph HI of the U.S. letter « DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, ... DHS promptly delete the sensitive EU PNR data ». Taking into account the responsibility of the air carriers in such collection of personal data, the safeguards ensured by in the U.S. letter may be considered adequate (4).

(c) Duration of PNR data retention

41. According to Paragraph VII of the U.S letter, « DHS retains EU PNR data in an analytical database for seven years, after which time the data will be moved to dormant, non-operational status » PNR data in « dormant » (non-operational) status are still available and they could be transferred, for instance, to other U.S. agencies or to third countries. Moreover, PNR data « in dormant status will be retained for eight years ». While the Agreement provides very little information in this regard, it appears that PNR data under dormant status will not be automatically processed, and access thereto is subject to certain more stringent safeguards. Therefore, from a legal point of view there is a clear difference between operational and non-operational status.

42. The period of retention could in practice be extended even further, as DHS states that they only « expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions ». The matter of the total possible duration of data retention therefore remains open.

43. In his Opinion of 22 November 2005, in the PNR case, Advocate General Léger took the view that, on the basis of the first PNR Agreement, « the normal length of time for which data from PNR are kept is three years and six months » and that « that period is not manifestly excessive bearing in mind in particular the fact that ... investigations which may be conducted following terrorist attacks or other serious crimes sometimes last several years » (5).

(1) Opinion of the Advocate General Léger in the TNR » Cases, paragraph 238, cited above.

(2) Council Framework Decision of 13 June 2002, OJ L164 of 22 June 2002, p. 3.

(3) See the Document of the Council of 30 November 2005 14469/4/05 REV 4 on the European Union Counter-Terrorism Strategy.

(4) Other information can be required by the DHS in the light of the special circumstances provided for in paragraph III, third subparagraph, of the DHS letter : « if necessary, in an exception case where the life of data subject or of others could be imperilled or seriously impaired, DHS officials may require and use information in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law ». In this case also, the guarantee provided for can be considered as adequate.

(5) Paragraph 242 of the Opinion of Advocate General Léger in the « PNR » case.

44. In the regime of the new PNR Agreement the normal length of time for the PNR data retention will be seven years. In the absence of objective criteria, it would be difficult to consider this period as being *prima facie* disproportionate. The reason that such a long period of data retention may be considered justified is the necessity of conducting investigations concerning terrorist attacks or other very serious crimes. The prevention of terrorism, as it is conceived in the U.S., can imply a long-term duration of the data retention. The storage and detention of data from PNR will be necessary not only for purposes of preventing and combating terrorism, but, more widely, for law-enforcement purposes (1). Article 5(e) of Convention 108 provides that personal data undergoing automatic processing shall be « preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ». In the fight against terrorism, seven years can be justified in principle as a proportionate duration for data retention.

45. Moreover, the declared intention of DHS to review the effect of the retention rules on operations and investigations based on its experience over the next seven years clearly indicates the will of the parties to take into account their experiences in the practical application of the Agreement to verify whether such a long period of data retention is justified in fact.

46. However, a problem exists concerning the retroactivity of the new PNR data retention period. according to the second subparagraph of Paragraph VII of the U.S. letter, the new retention periods « also apply to EU PNR data collected on the basis of the Agreements between the EU and the US, of May 28, 2004 and October 19, 2006 ». There are two aspects of the problem : the first one concerns the principle of non-retroactivity in international law, the second one the non-retroactivity in the application of administrative measures in a national legal order. Both of them are related to the principle of legal certainty.

47. Article 28 of the Vienna Convention on the Law of Treaties recognises the possibility for parties to conclude agreements providing some retroactive effects.

48. On the other hand, on the basis of Article 5(a) of Convention 108, data must be obtained and processed fairly and lawfully. Even if the criterion of lawfulness could be said to be complied with, the longer period of retention does not respect the legitimate expectations of those who provided their data under the previous regime that these would be stored for the period determined under that regime, and not under the 2007 PNR Agreement The retroactive application of the 2007 PNR Agreement could therefore be said to be unfair.

49. The Legal Service does not have any information as to the reasons for which the EU Council accepted such a provision amongst the assurances given by the DHS. Nevertheless, taking into account the situation created by the new PNR Agreement, the only possible solution to protect their rights for persons whom PNR data will be retained by the PHS for a longer period would be to address the U.S. judicial authority according to relevant U.S. law.

(d) Access to information and redress

50. Paragraph IV of the U.S. letter contains assurances by the DHS that it will extend administrative Privacy Act protections to PNR data, « including data that relates to European citizens ».

51. DHS has undertaken not to disclose PNR data to the public, except to the data subjects or their agents in accordance with U.S. law. DHS also maintain, in conformity with U.S. law, « a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information or correction of PNR » (2) Also, DHS ensures that « PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U.S. Privacy Act and the U.S. Freedom of Information Act (FOIA) » (3).

52. As it is pointed out in the U.S. letter, the FOIA permits any person, regardless of nationality or country of residence, access to a U.S. federal agency's records, except to the extent such records are protected from disclosure by an applicable exemption under the FOIA. The U.S. letter underlines that « under FOIA any requester has the authority to administratively and judicially challenge DHS's decision to withhold information ». Consequently, the availability of a judicial remedy under the FOIA constitutes in principle a significant safeguard with regard to the right to respect private life and personal data protection.

53. According to Paragraph V of the U.S. letter, « administrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records ». This assurance constitutes an important improvement in comparison with the Undertakings accompanying the first PNR Agreement. Insofar the rights guaranteed to EU citizens, concerned by the PNR data transfers, are the same ensured to the U.S. citizens.

(1) *Ibid.*

(2) These policies are accessible on the DHS website, *www.dhs.gov.*

(3) The FOIA defines administrative agency records subject to disclosure, mandatory disclosure procedures and exemptions to the statute.

54. Taking into consideration the general system established by the FOIA and conditions under which access is allowed to PNR data subjects, the level of protection ensured by U.S. law concerning access to information and redress can be considered adequate.

(e) Dissemination of PNR data

— Transfers to other U.S. agencies

55. The new PNR Agreement and the U.S. letter do not clearly identify the U.S. national services and agencies which may be entitled to receive and use passenger data. Unlike the Undertakings which accompanied the PNR Agreement of 2004, no mention is made to the so-called « Designated Authorities » and to the fact that DHS is considered to be the « owner » of the data.

56. According to the U.S. letter, « DHS shares EU PNR data only for the purpose named » in Paragraph I and must treat EU PNR data as sensitive and confidential in accordance with U.S. laws. However, DHS can, « at its discretion [provide] PNR data to other domestic government authorities with law enforcement, public security, or counterterrorism functions, in support of counterterrorism, transnational crime and public security cases [...] they are examining or investigating, according to law, and pursuant to written understandings and US. law on the exchange of information between US. government authorities ». The transfer to other U.S. agencies must be made on the basis of a case-by-case analysis, as the access must be strictly and carefully limited and be proportionate to the nature of the case. In any case, what is really essential is that the eventual treatment of PNR data by other U.S. agencies may only be made in conformity with U.S. law; it is the respect of this condition which would ensure the existence of an adequate level of protection.

57. The precautions provided for in Paragraph II of the U.S. letter do not clearly demonstrate that the level of protection of PNR data by the DHS in case of transfer to other U.S. agencies is inadequate.

— Transfers to third countries

58. The possible dissemination of PNR data to third countries is problematic. Clause 6 of the Agreement provides that the « EU will not interfere with relationships between the United States and third countries for the exchange of passenger information on data protection grounds ». according to the U.S. letter « EU PNR data is only exchanged with other government authorities in third countries after consideration of the recipient's intended uses(s) and ability to protect the information. Apart from emergency circumstances, any such exchange of data occurs pursuant to express understanding between the parties that incorporate data privacy protections comparable to those applied to EU PNR by DHS [...] ».

59. Unlike the Undertakings of the first PNR Agreement (1), Clause 6 of the new Agreement and the assurances given in the U.S. letter do not limit the transfer of PNR data to third countries to a case-by-case basis. The obligation not to interfere in any decision of the U.S. authorities to transfer PNR data to third countries has the consequence of depriving the EU of an effective control of such transfers and therefore of weakening the system of consenting these transfers where and when an adequate level of protection is ascertained.

60. Even if it is true that the adequate level of protection of personal data has been recognised for some third countries (2), this situation constitutes rather the exception than the rule in the relations between the EU and third countries. In accepting the above-mentioned provisions in the 2007 PNR Agreement, the Council has failed to reserve to the EU the possibility to deny onward transfers to third countries.

61. This was not the case, for instance, for the agreement concluded between the EU and Canada (3). The Commission Decision on the adequate protection of personal data contained in the PNR of air passengers transferred to the Canada Border Services Agency (CBSA) is based on the Commitments of the CBSA set out in the Annex of the Decision. In these commitments it is provided that the disclosure of Advance Passenger Information (API) and PNR information to other countries will be possible only with « an arrangement or agreement under subsection 8(2) of the Privacy Act and subsection 107(8) of the Custom Act » (4). This provision provides safeguards concerning the onward transfers of the PNR data, because Canada will recognise the existence of an adequate (or comparable) level of protection in a third country on the basis of its law, considered by the EU as giving an adequate level of protection.

(1) OJ L235 of 6 July 2004, p. 15.

(2) See, for instance, the Commission Decision of 30 June 2003 on the adequate protection of personal data in Argentina (OJ L168 of 5 July 2003, p. 19).

(3) See Council Decision 2006/230/EC of 18 July 2005 and the Agreement between the EC and the Government of Canada on the processing of Advance Passenger Information (API) and Passenger Name Record (PNR) Data (OJ L 82 of 21 March 2003, p. 14 and p. 15).

(4) See Commission Decision 2006/253/EC of 6 September 2005 and the Commitments by the CBSA (OJ L 91 of 29 March 2006, p. 49 and p. 53).

62. There are no rules in the 2007 PNR Agreement which oblige the U.S. to ascertain that the third countries to which PNR data are transferred guarantee a level of adequate protection. U.S. authorities will only consider the recipient's reasons for requesting the data and its ability to protect the information. These conditions are not necessarily sufficient to consider such transfers as being proportionate and acceptable.

63. The scope of the Agreement is widened as a result. The consequence of these possible transfers to third countries is that EU authorities and Member States will lose any kind of control over the PNR data. This clearly undermines the Council's finding of an adequate level of protection.

64. No sufficient reasons are given, in the EU letter, to assert that in transferring PNR data to third countries, the DHS ensures an adequate level of data protection. Assuming that the possible interference by a public authority with the exercise of the right to respect private life must be justified in accordance with the law and necessary in a democratic society, as prescribed by Article 8(2) of the ECHR, the adequacy declaration does not appear to comply with these requirements.

65. In the light of these considerations, the Legal Service takes the view that transfers of PNR data to third countries may constitute a violation of the principle of proportionality because, in the absence of a clear justification, they appear to go beyond what is necessary in order to achieve the declared objective of the 2007 PNR Agreement.

IV.B. The statement of reasons

66. In his letter, Mr Cavada has requested an evaluation of whether the decision on adequacy « could be considered adequately motivated11. As noted above, the Council statement on adequacy is contained in both clause 6 of the 2007 PNR Agreement and the EU letter.

67. As the Agreement is based on Titles V and VI of the EU Treaty, the normal requirement that Council acts « state the reasons on which they are based » does not apply. This follows from Articles 28 EU and 41 EU which exclude Article 253 EC from the list of provisions of the EC Treaty which apply to those Titles.

68. Even if opinion is divided on whether the requirement to state reasons applies as a general principle of law in this particular context, it is very widely recognised that the institution concerned must provide appropriate and sufficient reasons to justify any derogations from the protection of fundamental rights, including the protection of personal data, such as the dérogations contained in the 2007 PNR Agreement.

69. However, subject to the reservations expressed above concerning the retroactive effect of some provisions of the Agreement and transfers by the U.S. to third countries, it would be difficult to argue that the Agreement does not contain a sufficient statement of reasons. Recital (3) in the preamble of the Council Decision states that in the U.S. letter « DHS has offered assurances for the protection of PNR data transferred from the European Union concerning passenger flights to or from the United States ». The preamble to the Agreement demonstrates in some detail its purposes and the legal and political context in which it was concluded.

70. The 2007 PNR Agreement is based on the assurances given by the DHS. This situation necessarily implies that in case these assurances are not fully respected, the EU can determine, according to Clause 7 of the Agreement, that the U.S. has breached the Agreement. The consequence will be the termination of the Agreement and the revocation of the adequacy determination.

71. The reasons which would justify the adequacy finding are set out in particular in the assurances given in the « U.S. letter to EIF », to which clause 1 of the Agreement explicitly refers, and in the clauses of the Agreement which concern the treatment by the DHS of PNR data and related matters (see in particular Clauses 2 and 4).

72. Subject to the specific points outlined above, from a legal point of view, the statement of reasons can therefore be considered to be globally satisfactory.

IV.C. The review of the 2007 PNR Agreement and the principle of legal certainty

73. In his letter, Mr CAVADA raises the question of whether the arrangement for reviewing the Agreement creates a « special authority » and whether this could undermine legal certainty.

74. Clause 3 of the 2007 PNR Agreement provides that PNR data must be processed in accordance with applicable U.S. law. according to Clause 4 of the Agreement and paragraph X of the U.S. letter, DHS and theEU will periodically review the implementation of this Agreement, the DHS letter, and U.S. and EU PNR policies and practices with a view to mutually assuring the effective operation and privacy protection of their system. Paragraph X of the U.S. letter specifies that in the review, « EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate ». In addition, the « EU and DHS will mutually determine the detailed modalities of the review » and the « US. will

reciprocally seek information about Member States PNR systems as part of this periodic review, and representative of Member States maintaining PNR systems will be invited to participate in the discussion ».

75. In fact, the review is to be carried out by the Contracting Parties, namely the United States and the European Union. The EU Commissioner and the Secretary of Homeland Security are charged with reaching agreement on any review.

76. The penultimate paragraph of the Agreement stating that it « is not intended to derogate from or amend the laws of the United States of America or the European Union or its Member States » has to be understood in the sense that the Agreement will not have the legal effect of changing the U.S., EU or Member States » national rules on the protection of personal data. The purpose of the Agreement is only to authorise the processing and the transfer of PNR data in order to prevent and combat terrorism and transnational crime in a more effective way.

77. It follows that the 2007 PNR Agreement did not establish any « special authority » with responsibilities in the field of data processing and transfer of personal data. National rules of Member States are still in force and the rules concerning adequacy and their review provided for in the Agreement between U.S. and EU are, in principle, in conformity with Convention 108 and the Additional Protocol 181 to the extent that the adequate level of data protection is properly established.

IV.D. The alleged discrimination between European citizens in the application of criminal law by the U.S.

78. According to Mr CAVADA's letter, a problem could arise concerning discrimination between European citizens because of U.S. criminal jurisdiction. He considered this risk to be inherent with « the fact that the number of data transmitted to the US. authorities varies according to the number of data managed by each Airline » (1).

79. Even if there may be some differences as regards the number of data in fact made available by air carriers operating passenger flights, the U.S. administrative authorities, courts and tribunals will not extend their jurisdiction on the basis of the 2007 PNR Agreement. The purpose of this Agreement is only to ensure the availability of PNR data to the U.S. DHS. Therefore, the circumstance that the number of PNR data transmitted to the U.S. authorities can differ according to the number of data managed by each air carrier does not constitute in itself a relevant issue for the applicability of criminal laws.

80. U.S. criminal law is, by definition, different from that of the Member States of the EU. The existence Of different systems of personal data protection in relation to judicial and police activities does not imply discrimination between European citizens and, at any rate, it cannot be challenged before a judicial authority.

81. In our view, the Member States of the EU do not accept « a weakened penal protection » on the basis of the Agreement. The constitutional and criminal law protections ensured by the U.S. law have not been modified by this Agreement and by the adequacy statement of the EU Council. When flying to the U.S., European citizens are aware of the obligation to provide some information and personal data. Such citizens are in an objectively different legal situation compared to those who do not travel to the U.S., and any difference of treatment arising from the application to them of the U.S. criminal law cannot be deemed to result from illegal discrimination.

82. European citizens will not be subject to U.S. criminal law because of the 2007 PNR Agreement, but because of any infringement of the U.S. criminal law alleged to have been committed. In the latter case, any possible discrimination can be ascertained only by the competent U.S. judicial authorities.

IV.E. The relationship between the PNR agreement and other EU/U.S. Agreements (MLA — Extradition — Europol — Eurojust)

83. The Agreement on mutual legal assistance (MLA Agreement) between the European Union and the United States of America, signed on 25 June 2003 (2), is intended to enhance cooperation and mutual legal assistance between the European Union and he United States of America. Similarly, the Extradition Agreement, signed on the same day (3), seeks to enhance cooperation in the context of applicable extradition relations between the Member States and the United States.

(1) See the letter of 10 August 2007 of the chairman of LIBE Committee to the Jurisconsult, page 3.

(2) OJ L181 of 19 July 2003, p. 34.

(3) OJ L181 of 19 July 2003, p. 27.

84. The MLA Agreement applies to persons under investigation (1) for criminal offences, rather than air passengers. The data protection it provides are in fact less strict than that of the 2007 PNR Agreement, and it is clear that « generic restrictions » on the processing of personal datar such as those under the PNR Agreement, do not apply (2).

85. The Extradition Agreement does not contain any data provisions which could be assimilated with the relevant provisions of the 2007 PNR Agreement, and the question of a conflict does not therefore arise.

86. The Agreement between the U.S. and Europol (6 December 2001) is intended to enhance the cooperation between police authorities of EU Member States, acting through Europol, and U.S. authorities. It cannot be considered as having the same purpose of the PNR Agreement (3). Article 3(4) of the Supplemental Agreement between Europol and the United States on the exchange of personal data and related information, signed on 20 December 2002, provides that its application may not affect the application of « any other agreement or arrangement on the exchange of information between the Unites States and any Member States or institution of the European Union ». Consequently, in case of conflict, the PNR Agreement would prevail.

87. The Agreement between U.S. and Eurojust (6 November 2006) seeks to enhance cooperation between EU and U.S. prosecutors on terrorism and cross-border criminal cases. In order to achieve this purpose Eurojust and U.S. may exchange information in accordance with the procedure established in the Agreement (4). Provisions concerning the privacy and data protection and the limitation on use to protect personal and other data are included in the Agreement as well as specific provisions on data security, access to and correction and deletion of personal data and time limits for the storage of personal data (5). The purpose of the U.S./Eurojust Agreement being clearly different from that of the 2007 PNR Agreement, its specific provisions on privacy and data protection do not apply.

IV.F. Possibility of challenging the Council Decision on PNR Agreement before the Court of Justice

88. There are a number of grounds on which the compatibility of the 2007 PNR Agreement and the Council Decision authorising its conclusion with the generally recognised principles governing the protection of personal data.

89. As these two acts are based on the EU Treaty, the possibilities for challenging them before the Court of Justice are defined by Article 35 EU. It follows from this provision that *prima facie* the Court enjoys material jurisdiction to rule on the validity of the Council Decision, whether in the framework of a preliminary ruling requested by a national court (Article 35(1) to (3) EU) or in annulment proceedings (Article 35(6) EU).

90. In the present state of the Treaty, however, it is clear that the European Parliament is not empowered to bring annulment proceedings under the express terms of Article 35(6) EU. Such actions may only be initiated by a Member State or the Commission, Similarly, even if the validity of the Council Decision were challenged indirectly in a request for a preliminary ruling, Parliament would not be entitled to submit observations as of right on such a request, under the terms of Article 23 of the Statute of the Court of Justice, as the Council Decision was not adopted in codecision.

91. The Court has on occasion exercised its discretionary power to invite Parliament to submit observations in proceedings not involving the validity or interpretation of codecision acts. However to date it has only done so where a question had arisen concerning the internal functioning of Parliament, which is not the case here.

---

(1) These investigations can be made with a view to criminal prosecution or referral to criminal investigation or prosecution authorities.

(2) Article 9 of the MLA Agreement provides for limitations on use to protect personal data and other data, more specifically, Article 9, paragraph 2, subparagraph (b), provides that « generic restrictions with respect to the legal standards of the requesting State for processing personal data may not be imposed by the requested State as a condition under subparagraph (a) [additional conditions to give evidence or information] to providing evidence or information ». In the Explanatory Note on the MLA Agreement is stated that Article 9 (2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases and that « a broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded ». Even the fact the requesting and the requested States have different systems of protecting the privacy of data or have different means of protecting personal data « may as such not be imposed as additional conditions under Article 9(2)(a) ».

(3) See also the Mutual evaluation of the cooperation agreements Europol — United States in the council of the European Union document of 27 July 2005 (11502/05 LIMITE — EUROPOL 28).

(4) Eurojust has concluded Agreements also with other third countries, as Iceland, Romania and Norway.

(5) The exchange of information and data is made either between the liaison prosecutor and the national members concerned of the College of Eurojust (national members, judges, prosecutors of police officers) or directly between the prosecutorial authority and the national members concerned in the College.

92. It follows that at present there appears to be no avenue whereby Parliament could challenge the legality of the 2007 PNR Agreement. That said, it follows from Article 41 EU, which applies inter alia Article 197 EC to the area of police and judicial cooperation in criminal matters, and Article 39(3) EU that the Commission and the Council are obliged to answer questions put to the European Parliament in this area of Union activity. The committee may wish to consider inviting the other institutions to explain how the PNR Agreement can be said to comply with data protection principles in the light of the queries raised in Mr CAVADA's letter and the present opinion.

V. CONCLUSIONS

93. In the light of the foregoing, the Legal Service has reached the following conclusions :

(i) There are no specific criteria, either in the EU Treaty or in legislative acts, against which to judge the conformity of the 2007 PNR Agreement with the EU law. However, the Agreement itself refers to the protection of fundamental rights in accordance with Article 6(2) EU, as well as the right to the protection of personal data, which therefore provide the relevant criteria.

(ii) All the Member States are Parties to Council of Europe Convention 108 on the protection of individuals with regards to automatic processing of personal data, whose principles may be considered common to the Member States within the meaning of Article 6(2) EU.

(iii) Taking into account the specific purpose of the Agreement, the type and the number of data as well as the duration of the PNR data retention can be considered as proportionate for the achievement of the purpose of the Agreement.

(iv) The extension of the duration of the PNR data retention to the data collected under the previous PNR regime could constitute a violation of the principle of non-retroactivity and of the principle of legal certainty.

(v) Taking into consideration the general system established by the FOIA and conditions under which access is allowed to PNR data subjects, the level of protection ensured by the U.S. law concerning access to information and redress can be considered adequate.

(vi) The onward transfers of PNR data by the U.S. authorities to those of third countries could constitute a violation of the principle of proportionality, in the absence of clear justifications.

(vii) Subject to reservations on a number of specific points, the statement of reasons of the 2007 PNR Agreement can be considered, from a legal point of view, to be globally satisfactory.

(viii) The 2007 PNR Agreement does not *prima facie* create discrimination between European citizens because of the jurisdiction of the U.S. criminal laws.

(ix) There are no grounds for considering that the 2007 Agreement is inconsistent or contradicts the EU-U.S.A. Agreements on Mutual Legal Assistance, Extradition, Europol or Eurojust

(x) In the present state of EU law, there appears to be no avenue whereby Parliament could challenge the legality of the 2007 PNR Agreement. The Council and the Commission could nonetheless be invited to explain to Parliament how the Agreement could be said to comply with EU data protection principles in the light of the queries raised in Mr CAVADA's letter and the present opinion.