



EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Director General

Brussels, 09 NOV. 2011
home.a.3(2011)1220788

Mr Peter Hustinx
European Data Protection
Supervisor
Rue Wiertzstraat 60 (MO 63)
1047 Brussels

Subject: EU-United States PNR Agreement

Dear Mr Hustinx,

I am pleased to enclose the draft PNR agreement between the European Union and the United States of America.

U.S. legislation empowers the Department of Homeland Security (DHS) to require each air carrier operating passenger flights to and from the U.S., to provide it with electronic access to Passenger Name Record (PNR) data prior to the passenger arriving or leaving the U.S.. The requirements of the U.S. authorities are based on title 49, United States Code, section 44909c (3) and its implementing regulations (title 19, Code of federal regulations, section 122.49b).

This legislation aims at obtaining PNR data electronically in advance of a flight's arrival and therefore significantly enhances DHS ability to conduct efficient and effective advance risk assessment of passengers and to facilitate bona fide travel, thereby enhancing the security of the U.S.. The European Union in cooperating with the U.S. in the fight against terrorism and other serious transnational crime views the transfer of PNR data to the U.S. as fostering international police and judicial cooperation which will be achieved through the transfer of analytical information flowing from PNR data by the U.S. to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

The European Union signed an agreement in 2007 with the United States on the transfer and processing of PNR data based on a set of commitments by DHS in relation to the application of its PNR programme¹. The European Parliament issued a resolution

¹ OJ L204/16, 4.8.2007

criticising various aspects of the agreement, especially regarding the level of data protection².

Following the entry into force of the Lisbon Treaty and pending the conclusion of the agreement, the Council sent the 2007 U.S. Agreement to the European Parliament for its consent for the conclusion. The European Parliament adopted a resolution³ in which it decided to postpone its vote on the requested consent and requesting a renegotiation of the Agreement on the basis of certain criteria. Pending such renegotiation, the 2007 Agreement would remain provisionally applicable.

On 21 September 2010, the Council received a recommendation from the Commission to authorise the opening of negotiations for an Agreement between the European Union and the United States of America for the use and transfer of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime. On 2 December 2010, the Council adopted a Decision, together with a negotiation directive, authorising the Commission to open negotiations on behalf of the European Union.

Following negotiations the parties reached a draft agreement on 28 October 2011. The purpose of the Agreement is to ensure the availability of European passenger information, known as Passenger Name Record or PNR data to the U.S. Department of Homeland Security pursuant to which its services assess the risk a passenger may pose to the security of the U.S..

This draft agreement takes into consideration and is consistent with the general criteria laid down in the Communication from the Commission on the Global Approach to the transfer of Passenger Name Record (PNR) data to third countries and the negotiating directives given by the Council.

PNR has proven to be a very important tool in the fight against terrorism and serious crime. The Agreement has secured several important safeguards for those whose data will be transferred and used. In particular, the purpose of processing of PNR data is strictly limited to preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime. The retention period of the PNR data is limited and PNR will be used for a shorter period in the fight against serious transnational crime and a longer one for terrorism. In addition, the data will be depersonalised after the short period of 6 months. Individuals are provided with the right to access, correction, redress and information. The 'push' method of transfer is recognised as the only mode of transfer, with which all carriers will need to comply within 2 years of the Agreement. Sensitive data is to be used in very exceptional cases and deleted after a very short timeframe. Compliance with these rules shall be subject to independent review and oversight by various Department Privacy Officers, as well as by the DHS Office of Inspector General, the Government Accountability Office and the U.S. Congress.

Please find attached a proposal for a Decision from the Commission to the Council to sign the Agreement and a proposal for a Decision from the Commission to the Council to conclude the Agreement.

² P6_TA(2007)0347, 12.7.2007

³ P7_TA-(2010)0144, 5.5.2010

A result on this Agreement is expected in time for the November EU-US summit and the European Parliament is eagerly awaiting these proposals. It is for this reason that the Commission has launched a fast track inter-service consultation.

The Commission inter-service consultation is currently ongoing. You will find the draft proposals enclosed for your consultation, in line with your competence as supervisory authority of the Community institutions and bodies in relation to the processing of personal data pursuant to Article 286 of the EC Treaty and the note of the Commission's Secretary General of 15.02.2006 on the advisory role of the EDPS [CD/D(2005)1612].

I should be grateful, if you could send your opinion by 11.11.2011 midday the latest. I would ask that your opinion takes account of the fact that the proposal and the annexed Agreement, despite not having a formal classification, are politically very sensitive and should be treated as highly confidential. The person responsible for this file is

[REDACTED]

Yours sincerely,



Stefano Manservigi

Copy: Mr Philippe Renaudiere, Secretariat General



EUROPEAN COMMISSION

Brussels, XXX
[...] (2011) XXX draft

Proposal for a

COUNCIL DECISION

**on the signature of the Agreement between the United States of America and the
European Union on the use and transfer of Passenger Name Records to the United
States Department of Homeland Security**

EXPLANATORY MEMORANDUM

U.S. legislation empowers the Department of Homeland Security (DHS) to require each air carrier operating passenger flights to and from the U.S., to provide it with electronic access to Passenger Name Record (PNR) data prior to the passenger arriving or leaving the U.S.. The requirements of the U.S. authorities are based on title 49, United States Code, section 44909c (3) and its implementing regulations (title 19, Code of federal regulations, section 122.49b).

This legislation aims at obtaining PNR data electronically in advance of a flight's arrival and therefore significantly enhances DHS ability to conduct efficient and effective advance risk assessment of passengers and to facilitate bona fide travel, thereby enhancing the security of the U.S.. The European Union in cooperating with the U.S. in the fight against terrorism and other serious transnational crime views the transfer of PNR data to the U.S. as fostering international police and judicial cooperation which will be achieved through the transfer of analytical information flowing from PNR data by the U.S. to the competent Member States authorities as well as Europol and Eurojust within their respective competences.

PNR is a record of each passenger' travel requirements which contains all information necessary to enable reservations to be processed and controlled by air carriers.

Air carriers are under an obligation to provide the DHS with access to certain PNR data contained in the air carrier's automated reservation and departure control systems.

The data protection laws of the EU do not allow European and other carriers operating flights from the EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data without adducing appropriate safeguards. A solution is required that will provide the legal basis for the transfer of PNR data from the EU to the U.S. as a recognition of the necessity and importance of the use of PNR data in the fight against terrorism and other serious transnational crime, whilst avoiding legal uncertainty for air carriers. In addition, this solution should be applied homogenously throughout the European Union in order to ensure a legal certainty for air carriers and respect of individuals' rights to the protection of personal data as well as their physical security.

The European Union signed an agreement in 2007 with the United States on the transfer and processing of PNR data based on a set of commitments by DHS in relation to the application of its PNR programme¹.

Following the entry into force of the Lisbon Treaty and pending the conclusion of the agreement, the Council sent the 2007 U.S. Agreement to the European Parliament for its consent for the conclusion. The European Parliament adopted a resolution² in which it decided to postpone its vote on the requested consent and requesting a renegotiation of the Agreement on the basis of certain criteria. Pending such renegotiation, the 2007 Agreement would remain provisionally applicable.

On 21 September 2010, the Council received a recommendation from the Commission to authorise the opening of negotiations for an Agreement between the European Union and the

¹ OJ L204/16, 4.8.2007

² P7_TA-(2010)0144, 5.5.2010

United States of America for the use and transfer of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime.

On 11 November 2010, the European Parliament adopted a resolution on the Recommendation from the Commission to the Council to authorise the opening of the negotiations.

On 2 December 2010, the Council adopted a Decision, together with a negotiation directive, authorising the Commission to open negotiations on behalf of the European Union. Following negotiations between the parties, the Agreement was initialled on ...November 2011.

This Agreement takes into consideration and is consistent with the general criteria laid down in the Communication from the Commission on the Global Approach to the transfer of Passenger Name Record (PNR) data to third countries³ and the negotiating directives given by the Council.

PNR has proven to be a very important tool in the fight against terrorism and serious crime. The Agreement has secured several important safeguards for those whose data will be transferred and used. In particular, the purpose of processing of PNR data is strictly limited to preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime. The retention period of the PNR data is limited and PNR will be used for a shorter period in the fight against serious transnational crime and a longer one for terrorism. In addition, the data will be depersonalised after the short period of 6 months. Individuals are provided with the right to access, correction, redress and information. The 'push' method of transfer is recognised as the only mode of transfer, with which all carriers will need to comply within 2 years of the Agreement. Sensitive data is to be used in very exceptional cases and deleted after a very short timeframe. Compliance with these rules shall be subject to independent review and oversight by various Department Privacy Officers, as well as by the DHS Office of Inspector General, the Government Accountability Office and the U.S. Congress.

The Article 218(5) of the Treaty on the Functioning of the European Union states that the Council shall authorise the signing of international agreements.

The Commission therefore proposes to the Council to adopt a decision to sign the Agreement between the European Union and the United States of America on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security.

³ COM(2010)492.

Proposal for a

COUNCIL DECISION

on the signature of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 82(1)(d) and 87(2)(a), in conjunction with Article 218 (5) thereof,

Having regard to the proposal from the European Commission,

Whereas:

- (1) On 2 December 2010, the Council adopted a Decision, together with negotiation directives, authorising the Commission to open negotiations on behalf of the European Union between the European Union and the United States of America for the transfer and use of Passenger Name Records (PNR) to prevent and combat terrorism and other serious transnational crime.
- (2) The Agreement has been negotiated. The negotiations were successfully concluded by the initialling of the agreement.
- (3) The Agreement should be signed subject to its conclusion at a later date.
- (4) This Agreement respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, notably the right to private and family life, recognised in Article 7 of the Charter, the right to the protection of personal data, recognised in Article 8 of the Charter and the right to effective remedy and fair trial recognised by Article 47 of the Charter. This Agreement should be applied in accordance with those rights and principles.
- (5) [In accordance with Article 3 of the Protocol 21 on the Position of the United Kingdom and Ireland in respect of the area of Freedom, Security and Justice annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, the United Kingdom and Ireland take part in the adoption of this Decision.]
- (6) In accordance with Articles 1 and 2 of the Protocol 22 on the Position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Decision and is not bound by the Agreement or subject to its application,

HAS ADOPTED THIS DECISION:

Article 1

The signing of the Agreement between the European Union and the United States of America on the use and transfer of Passenger Name Records to the United States Department of Homeland Security is hereby approved, subject to its conclusion at a later date.

The text of the Agreement to be signed is attached to this Decision.

The Commission is authorised to designate the persons empowered to proceed to the signature, subject to its conclusion.

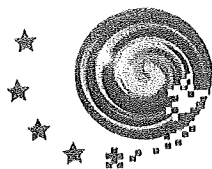
Article 2

This Decision shall enter into force on the day of its adoption.

Done at Brussels,

*For the Council
The President*

ANNEX



EUROPEAN DATA
PROTECTION SUPERVISOR

PETER HUSTINX
SUPERVISOR

Mr Stefano MANSERVISI
Director-General
DG Home Affairs
European Commission
BRU-LX46 06/105
B-1049 Brussels

Brussels, 11 November 2011
PH/ACL/kd D(2011)1993 C2011-1020

CONFIDENTIAL

Dear Mr Manservisi,

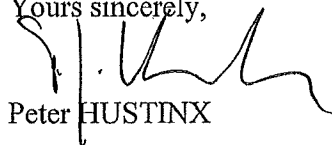
I am writing to you in reply to your letter of 9 November concerning the draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security (DHS).

We understand that the consultation of the EDPS takes place in the context of a fast track procedure.

Please find attached our preliminary comments on the draft Agreement. They are without prejudice to the formal Opinion that may follow under Article 28(2) of Regulation 45/2001. In that Opinion, also other relevant elements may be discussed.

Our services remain available, should you need any clarification in relation with this note.

Yours sincerely,



Peter HUSTINX

Cc: Ms Boulanger, Head of Unit - DG JUST data protection
Mr Renaudière, Commission Data Protection Officer

Contact persons: [REDACTED]

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

EDPS comments on the draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security (DHS).

Introduction

The proposed agreement between the EU and the US on PNR data is aimed at providing a solid legal basis for the transfer of PNR data to the US, which currently takes place on the basis of the provisionally applied 2007 agreement. The new agreement is expected to provide more legal certainty for air carriers and individuals on whom data are processed as well as enhanced safeguards as concerns the respect of individuals' rights to the protection of personal data.

As we underlined in previous comments on other PNR schemes, we note that this agreement is put forward in the context of a wider approach to PNR, which includes negotiations with third countries, global PNR guidelines and setting-up an EU-PNR scheme. The EDPS has closely followed these developments and has adopted two Opinions on the "PNR package" of the Commission and the Proposal for a Directive on EU-PNR¹.

Moreover, the Article 29 Working Party adopted a number of Opinions² underlining the specific data protection guarantees that should be included in an EU-US PNR agreement, which should have helped guiding the drafting of the new agreement. Several objections remain valid in the present draft agreement, which are developed below.

A preliminary and consistent remark reiterated in EDPS and Article 29 Working Party Opinions relates to the necessity and proportionality of the PNR scheme, which have not been sufficiently demonstrated.

[REDACTED]

The specific comments below are without prejudice to this preliminary and fundamental observation. We welcome the provisions which foresee specific guarantees such as data security, and those detailing enforcement and oversight. At the same time, we express concern about the scope of definitions and the conditions of retention of data.

¹ - Opinion of the EDPS of 25 March 2011 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;

- Opinion of the EDPS of 19 October 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries.

Both opinions are available at <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation>

² The opinions of the Article 29 Working Party are available at the following link: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

See in particular:

- Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, 14 June 2006, WP 122;

- Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, 27 September 2006, WP 124; and

- Opinion N° 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, 17 August 2007, WP 138.

[REDACTED]

Specific comments on the Proposals

○ Purpose and definitions

We welcome the fact that the purposes for which PNR data can be processed are precisely defined in Article 4 of the proposed agreement. The EDPS has always insisted on the importance of a strictly defined purpose limitation.

In particular, we note that Article 4(1)(a) generally provides for concrete elements which help to characterise "terrorist offences and related crimes"; for example, they may consist of conduct involving a violent act or act dangerous to human life, property or infrastructure. Although these definitions are not as precise as in the EU-PNR Proposal, they however help provide clarity and legal certainty. We however note that Article 4(1)(a)(2) is far less specific when it refers to conducts that "appear to be intended to" intimidate persons and affect or influence governments by intimidation or coercion (Article 4(a)(2)). We consider that more precision is needed in relation to the notion of "appear to be intended", which is a very open concept and might include a wider kind of politically motivated activities. Moreover, there is no limitation on what "appears" to a law enforcement officer to be intended - this should be limited by limiting words such as "manifestly" or at least "reasonably". The notions of "intimidating", "influencing" and "coercing" should also be clarified.

The possibility to process data in other exceptional cases raises additional questions, especially as it extends to "a serious threat and for the protection of vital interests of any individual". It is essential that such an extension of purpose be assessed on a case-by-case basis, and that the notion of "serious threat" be clarified. Moreover, we strongly question the use and processing of data "if ordered by a court". This is not in line with the purpose limitation principle and the principle according to which limitations to rights and freedoms must be foreseen by law⁴.

Article 4(3) should clarify that only the persons who are suspected of having taken part in any of the offences listed in Article 1 may be subject to closer questioning or examination. If no such precision is added, this would lead to an extension of the purposes followed to any kind of border control not related to serious crime and prevention of terrorism.

We also note that the list of PNR data annexed to the Proposals contains 19 types of data similar to the ones included in the 2007 agreement, which were already considered as disproportionate by the Article 29 Working Party⁵. This list contains too many open fields, which might include sensitive data, the processing of which is in principle prohibited under EU data protection law. This list should be considerably narrowed, in particular by specifying in detail the exact types of data to be processed wherever there are open data fields (e.g. in respect of "all available contact information", "all baggage information", "general remarks", etc.).

○ Sensitive data

We regret that the processing of sensitive data has not been fully excluded and that retention and residual use of sensitive data by the DHS is permitted.

⁴ Article 52(1) of the Charter of Fundamental Rights of the European Union.

⁵ Opinion N° 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, 17 August 2007, WP 138.

We take note that an automated system shall be implemented by DHS to filter and mask out sensitive data. It is not clear for how long the 'masked out' data are retained. Even if 'masked out', these data remain sensitive data, the processing of which is prohibited as a principle under EU data protection law. We reiterate our position that we do not support the filtering of sensitive data by DHS but a filtering at the source, and we therefore strongly recommend that sensitive data are filtered out by the air carriers before communicating them to DHS.

- Data security

Article 5 of the proposed agreement includes a comprehensive provision on data security and integrity, which is welcome. We welcome in particular the obligation to notify the affected individuals of a privacy incident. However, we consider that DHS should also be obliged to report security breaches to a competent US authority. It should also be clarified how DHS will report these breaches to the European authorities, in particular which types of breaches shall be notified (what does "significant privacy incidents" mean?) and to whom (who are the "relevant European authorities"?). We consider that Data Protection Authorities would in any case be a relevant recipient of this kind of information and should be included in the Proposal.

We welcome that all access to PNR and its processing and use shall be logged or documented by DHS. This will notably allow possible verification of whether the DHS has made appropriate use of the PNR data.

- Transfers by air carriers and 'push' method

We welcome that the 'push' method of transfer is recognised as the only mode of transfer, as stated in Article 15 of the proposed agreement. However, in view of the concerns underlined recently by the Article 29 Working Party⁶ in this respect, we strongly advise that the agreement expressly prohibits the possibility for US officials to separately access the data. This concern is particularly important as Article 15(5) seems to envisage the transfer of data through other means in certain circumstances; we insist that in no circumstances should it be permitted for US officials to have direct access to the databases of air carriers and to pull the data.

Furthermore, we consider that the transitory period of 2 years for air carriers to implement the 'push' system is too long and that the obligation to push data should become fully binding as of the entry into force of the agreement. Already for a number of years efforts have been made to phase out the pull method and we see no reason why a new additional transition period is needed.

According to Article 15, additional transfers should take place "for a fixed number of routine and scheduled transfers are specified by DHS". We consider that the number and periodicity of such transfers should be defined in the agreement. To enhance legal certainty, the conditions in which additional transfers would be allowed should also be more detailed.

⁶ Letter dated 19 January 2011 from the Article 29 Working Party addressed to Commissioner Malmström regarding the EU PNR Agreements with the US, Canada and Australia.

- Supervision and enforcement

The system of supervision, including oversight and accountability measures and insisting on the absence of discrimination based on nationality or place of residence, is welcome. The right of every individual to administrative and judicial redress is strongly supported, although we underline that the right to "judicial review" in the US is not exactly the same as the right to an effective judicial redress as is understood in the EU. We consider the role of DHS and in particular the DHS Chief Privacy Officer as particularly central in ensuring data subjects' rights and in guiding them in seeking administrative and judicial redress under US law. However, considering the complexity of the system, we consider that the EU and national data protection authorities should continue working with DHS on their procedures and modalities regarding data subjects' rights in order to ensure that these rights can be effectively exercised in practice.

- Retention of data

We consider the length of the data retention period as foreseen in Article 8 as one of the major difficulties in the proposal. A total retention period of 15 years is foreseen, with an initial 5 year retention period in an active database followed by up to 10 years storage in a dormant database. The length of the data retention is clearly disproportionate, applying EU standards, as was already underlined by the Article 29 Working Party⁷.

Even if data are masked out after a period of 6 months, the data are not fully anonymised and they can therefore be linked to an identified individual for as long as any direct or indirect identifiers are retained. We consider that the complete (i.e. irreversible) anonymisation of all data should take place, if not immediately after analysis, after 6 months as a maximum.

We consider that the necessity of the retention period should be further evaluated in respect of the whole retention period of 15 years, notwithstanding whether the data are kept in active or dormant databases. It might also be advisable to consider further limiting access rights, while data are still in an active database, subject to special authorisations.

- Onward transfers

The guarantees provided in Articles 16 and 17 are welcome, although we consider that the types of authorities who can receive PNR data should be further clarified and a list of possible domestic recipients drawn up.

We note that the level of the safeguards adduced by the recipients may be "equivalent or comparable" to the original agreement for domestic transfers, and regret that they are only "comparable" in case of transfers to third countries. We emphasise that any onward transfers by DHS to other recipients, whether in the US or to third countries, should only take place if the recipient adduces safeguards that are not less stringent than the ones set forth in this agreement. It should also be clarified in the agreement that the transfer of PNR data shall be done on a case-by-case basis, ensuring that only the necessary data will be transferred to the relevant recipients. In addition, we suggest that data transfers to third countries are subject to a prior judicial authorisation.

⁷ See footnote 5.

Finally, the Proposals foresee that when data of a resident of an EU Member State are transferred to a third country, the competent authorities of the Member State concerned should be informed where the DHS is aware of this situation. It is unclear why in some cases the DHS would not be aware of such a transfer. This point should be clarified and justified. We consider that further details should be included explaining the purpose for such a transmission to a Member State. Should such a transmission of information have an impact on the data subject, additional justification and safeguards should be included.

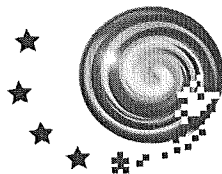
- Form and review of the agreement

It is not clear what is the legal form chosen by the US for entering into this agreement and how this agreement will become legally binding in the US. This should be clarified in the agreement.

We strongly believe that the new agreement should have immediate effect and that it should also apply to data collected under the July 23 and 26, 2007 agreement. Should the July 23 and 26, 2007 agreement continue to apply to the data collected under its terms, as is stated in Article 27(2) of the agreement, this would result in legal uncertainty and doubts especially with regard to the exercise of rights by individuals.

As concerns the modalities of the review, we welcome that clear modalities have been set out. However, for the review to be credible, we consider that Data Protection Authorities should be explicitly included in the review team.

Finally, we suggest that the review also concentrates on assessment of the necessity of the measures, on the effective exercise of data subjects' rights, and includes the verification of the way data subjects' requests are being processed in practice, especially where no direct access has been allowed.



EUROPEAN DATA
PROTECTION SUPERVISOR

PETER HUSTINX
SUPERVISOR

Mr Stefano Manservigi
Director-General
DG Home Affairs
European Commission
B-1049 Brussels

Brussels, 7 July 2010
PH/ACL/sk D(2010)1080 **C2010-0471**

Dear Mr Manservigi,

I am writing to you in reply to the letter of 22 June 2010 received from Mr Jonathan Faull concerning the draft Communication on the transfer of Passenger Name Record (PNR) data: a global EU approach - The next steps, and the proposals for Recommendations to authorise the Commission to (re) negotiate Agreements between the EU and respectively Australia, Canada and the United-States.

I welcome the informal consultation of the EDPS at this stage of the procedure.

You will find attached a note developing comments on both the Draft Communication and the proposals for Recommendations. This note consists of preliminary comments. It is without prejudice to the formal opinion that may follow under Article 28 (2) of Regulation 45/2001. In that opinion, also other relevant elements of the proposal might be discussed.

My services remain available, should you need any clarification in relation with this note.

Yours sincerely,

Peter Hustinx

cc. Mr Renaudière (Commission, Data Protection Officer)

Contact person: . [REDACTED]

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu

Tel.: 02-283 19 00 - Fax : 02-283 19 50

EDPS comments on the Communication from the Commission on the transfer of Passenger Name Record (PNR) data: a global EU approach - The next steps,

and on the Recommendations from the Commission to the Council to authorise the Commission to open negotiations for the conclusion of Agreements between the EU and respectively Australia, Canada and the United-States for the transfer and use of PNR data to prevent and combat terrorism and other serious transnational crime.

Introduction

As a preliminary comment, we welcome the horizontal approach of the Communication, in line with the recent requests of the Parliament for a thorough analysis and coherent view on existing and foreseen PNR schemes. A high and harmonised level of protection applicable to all these schemes is an objective which should be strongly supported.

We have doubts, nevertheless, as to the scope and the timing of the initiative: while the Communication mentions international agreements on PNR schemes *and* initiative for an EU PNR, the proposed standards included in the Communication relate only to international agreements. The EU framework will be discussed and developed in a later stage, most likely in the beginning of 2011.

A more logical agenda would in our view include a reflexion on a possible EU scheme including data protection safeguards compliant with the EU legal framework, and on this basis, develop an approach for agreements with third countries.

Let us also emphasise the ongoing work being done in relation with an EU-US general agreement on law enforcement, the purpose of which is to establish a set of reference principles guaranteeing a high level of protection for personal data as a condition to the exchange of such data. We consider that the outcome of the EU-US negotiations should be a reference for further bilateral agreements, including the PNR agreement with the US.

As a last introductory remark, we question the extent to which precise safeguards and conditions should be detailed in the standards developed in the Communication or in the guidelines established per country: if the overall objective is to harmonise the conditions of processing and exchange of PNR data, we consider that the margin of manoeuvre for each international agreement should be as limited as possible, and that the standards should set a precise framework. The standards should have an effective impact on the content of the agreements. Several comments below raise the need for more precision in that sense.

Specific comments on the communication

- Preliminary observation: Legitimacy of the scheme

The EDPS has already questioned in several occasions the need for a clear justification to the development of PNR schemes, be it within the EU or in order to exchange data with third countries. The necessity of the measures must be established and balanced with the degree of intrusion in the private life of individuals. The fact that recent technological developments now render wide access and analysis possible, as stated on page 4 *in fine*, is not in itself a justification to the development of the system.

The fact that data about innocent people are transferred in bulk to third countries raises serious proportionality issues, considering all the more that these data are then used for risk analysis purposes. Such a risk analysis performed on innocent people constitutes proactive measures, as is explicitly stated in the communication with following words: "use in order to

prevent a crime, survey or arrest persons before a crime has been committed"¹. Such proactive measures are traditionally used in strictly defined circumstances. Their use on a wide scale involving the screening of all passengers raises the question of compliance with fundamental data protection principles, including Article 8 of the ECHR, Articles 7 and 8 of the Charter and Article 16 of the TFUE.

Any final decision on the legitimacy of PNR schemes should take into account these elements, which should be analysed and developed in the impact assessment now being conducted in the framework of the EU PNR project. The agenda should be set in order to allow the taking into account of the results of this impact assessment in the drafting of global requirements for PNR schemes.

- Content of the proposed standards

We welcome the extensive list of standards, visibly inspired by EU data protection principles, and which in several aspects should strengthen the protection foreseen in specific agreements. The added value and shortcomings identified in these standards are listed hereafter.

- Binding character of any agreement:

Although we support the need to establish clearly the binding character of agreements for all parties concerned, we believe this should be complemented by an explicit indication that the agreements shall ensure *directly enforceable rights* to data subjects. This statement should also be mentioned in the guidelines for each separate agreement.

- Appreciation of adequacy:

The assessment of adequacy is to be made in the light of "all circumstances" including also compliance with "international standards". The nature of those international instruments could be detailed, as it is not clear whether it is intended to take into account in the assessment new developing initiatives such as the international data protection standards elaborated by Data Protection Authorities² or the ISO work on a standard on security and privacy³.

- Scope and purpose:

The first two points in the list of principles relate to purpose limitation. Under the subtitle "use of data", the first point mentions law enforcement and security purposes, and further refers to terrorism and other serious transnational crimes, as based on the "approach of" definitions laid down in EU instruments. We question the meaning of such a wording which could lead to think that future agreements would not be based precisely on these definitions but would be inspired by them. To avoid any misunderstanding, we advise to delete the words "approach of".

The second point seems to refer more to the scope (the nature of data collected) than to the purpose principle. The list of data which can be transferred mirrors to a very large extent the US PNR list, which has been criticized as being too extensive in several opinions of the Article 29 Working Party⁴. We consider that this list should be reduced in accordance with the opinion of the Working Party, and that any addition be duly justified. This is the case especially for the field "general remarks".

¹ Page 4 of the Communication, chapter 3.1.

² Resolution welcoming the International Standards on the Protection of Personal Data and Privacy adopted in Madrid at the occasion of the International Data Protection and Privacy Commissioners' conference, 4-6 November 2009.

³ Project 29100. Information technology - Security techniques - Privacy framework.

⁴ Opinion of 23 June 2003 on the Level of Protection ensured in the United States for the Transfer of Passengers' Data, WP78. This opinion and subsequent opinions of the Working Party on this issue are available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

- Sensitive data:
The Communication indicates that these data shall not be processed "in principle". Does that mean that exceptions are still possible? In our view this possibility should be clearly excluded. Allowing for the processing of sensitive data, even in limited cases, would align the level of protection of protection of all PNR schemes on the less data protection compliant scheme rather than on the most compliant. The words "in principle" should therefore be deleted. This comment is also valid for the guidelines.
- Enforcement:
We welcome the system of supervision as foreseen in the communication, including oversight and accountability measures. The right of every individual to administrative and judicial redress is also strongly supported. As far as access rights are concerned, we understand that no limitation can be foreseen, which is welcome. Would a limitation be necessary in exceptional cases, its precise scope and the necessary safeguards including indirect right of access should be clearly mentioned in the standards.
- Automated individual decisions:
Such decisions are allowed as long as they do not produce "significant adverse actions concerning the relevant interests of the individuals". We question the exact scope of this provision, and in particular the notion of "significant" adverse action. To avoid any flexible interpretation of this provision, the standards should prohibit any automated decision which produces adverse actions or effects on an individual.
- Onward transfers:
We welcome the restriction of any onward transfer, be it to other government authorities or to third countries, on a case by case basis. With regard to the level of protection afforded by the recipient, we question however the difference in wording: for other authorities the level of protection must be "the same" while for third countries it should be "equivalent". We think that similar wording should be used in both cases, which means that "the same" level protection should always be afforded. Alternatively, an "adequate" level of protection could be used for third countries, which would guarantee more legal certainty that "equivalence".
- Need for more precision and harmonisation:
Chapters on the modalities of transmission and on overarching concepts would benefit from more precision. Some aspects, like the period of retention of data, are not harmonised at all. The frequency of transmissions by airlines ("reasonable"), as well as the duration of agreements ("fixed", "appropriate") and their review ("periodical") should be defined. Existing schemes providing for the most privacy compliant provisions should be the benchmark for such exercise.

[REDACTED]

Conclusion

The elaboration of a global approach on the transfer of passenger data is in our view an essential prerequisite to the revision of the existing agreements with third countries and to the possible development of an EU PNR system. We support the work conducted by the Commission in this view, with the following caveat:

- The elaboration of an impact assessment for an EU PNR should constitute one of the key elements of the global picture.
- The standards developed in the communication should be as precise as possible in order to limit the margin of manoeuvre of specific PNR schemes and to guarantee a harmonised and strong level of protection. This should be the case especially with regard to the purpose and scope of the PNR schemes, the question of automated decisions, onward transfers, the exercise of the rights of data subjects, the period of retention and the general oversight. The most privacy compliant practice in existing schemes should be the basis for a harmonised framework.