Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion 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

(2012/C 35/03)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]),

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 41 thereof ([2]),

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS and aim of the Opinion

1. On 28 November 2011, the Commission adopted a proposal for a Council Decision on the conclusion of the 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 ([3]) (hereinafter: 'the agreement').

2. On 9 November 2011, the EDPS was consulted informally on the draft proposal, in the context of a fast track procedure. On 11 November 2011, he issued a number of restricted comments. The aim of the present Opinion is to complement these comments in light of the present proposal and to make his views publicly available. This Opinion also builds on a number of earlier interventions by the EDPS and the Article 29 Working Party in relation to PNR.

1.2. Context of the proposals

3. The agreement aims at providing a solid legal basis for the transfer of PNR data from the EU to the US. The transfer is currently based on the 2007 agreement ([4]) because the Parliament decided to postpone its vote on the consent until its data protection concerns were met. In particular, in its resolution of 5 May 2010 ([5]), the Parliament referred to the following requirements:

([1]) OJ L 281, 23.11.1995, p. 31.
([2]) OJ L 8, 12.1.2001, p. 1.
([3]) COM(2011) 807 final.
([4]) 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 (DHS) (OJ L 204, 4.8.2007, p. 18).
([5]) European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada (OJ C 81E, 15.3.2011, p. 70). See also European Parliament resolutions of 13 March 2003 on transfer of personal data by airlines in the case of transatlantic flights (OJ C 61 E, 10.3.2004, p. 381), of 9 October 2003 on transfer of data by airlines in the case of transatlantic flights: state of negotiations with the USA (OJ C 81 E, 31.3.2004, p. 105), of 31 March 2004 on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (OJ C 103 E, 29.4.2004, p. 665), recommendation to the Council of 7 September 2006 on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime (OJ C 305 E, 14.12.2006, p. 250), resolution of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (OJ C 287 E, 29.11.2007, p. 349), and resolution of 12 July 2007 on the PNR Agreement with the United States of America (Texts adopted, P6_TA(2007)0347). All available on http://www.europarl.europa.eu

— compliance with data protection legislation at national and European level,

— a privacy impact assessment prior to the adoption of any legislative instrument,

— a proportionality test demonstrating that existing legal instruments are not sufficient,

— strict purpose limitation ([6]) and limitation of the use of PNR data to specific crimes or threats, on a case-by-case basis,

— limitation of the amount of data to be collected,

— limited retention periods,

— prohibition of data mining or profiling,

— prohibition of automated decisions significantly affecting citizens ([7]),

— appropriate mechanisms for independent review, judicial oversight and democratic control,

— all international transfers should comply with EU data protection standards and be subject to an adequacy finding.

4. The present agreement must be considered in the context of the global approach to PNR, which includes negotiations with other third countries (namely Australia ([8]) and Canada ([9])), and a proposal for a PNR scheme at the EU level ([10]). It also falls within the scope of the current negotiations for an agreement between the EU and the US on the exchange of personal data in the framework of police and judicial cooperation in criminal matters ([11]). In a wider context, the agreement has been initialled a few weeks before the expected adoption of the proposals for the review of the general data protection framework ([12]).

5. The EDPS welcomes this global approach aiming at providing a coherent legal framework for PNR agreements in line with EU legal requirements. However, he regrets that this timing does not allow in practice to ensure the consistency of these agreements with the new EU rules on data protection. He would also like to recall that the general agreement between the EU and the US on data exchanges should be applicable to the EU-US PNR Agreement.

([6]) Limited to law enforcement and security purposes in cases of organised and transnational serious crime or terrorism of a cross-border nature, on the basis of the legal definitions laid down in Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3) and in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant (OJ L 190, 18.7.2002, p. 1).

([7]) 'No "no-fly" decision or decision to investigate or prosecute may ever be taken on the sole results of such automated searches or browsing of databases'.

([8]) Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, signed on 29 September 2011.

([9]) Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data (OJ L 82, 21.3.2006, p. 15).

([10]) 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 (COM/2011/0032 final).

([11]) On 3 December 2010, the Council authorised the opening of the negotiations for an agreement between the EU and the US on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters. See Commission press release on http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661

([12]) See Commission communication on a comprehensive approach on personal data protection in the European Union, 4 November 2010, COM(2010) 609 final, and its follow-up.

2. GENERAL REMARKS

6. According to the EU Charter of Fundamental Rights, any limitation to fundamental rights and freedoms must be necessary, proportional and laid down by law. As repeatedly stated by the EDPS ([13]) and the Article 29 Working Party ([14]), the necessity and proportionality of the PNR schemes and of the bulk transfers of PNR data to third countries have so far not been demonstrated. The European Economic and Social Committee and the Fundamental Rights Agency also share this view ([15]). The specific comments below are without prejudice to this preliminary and fundamental observation.

7. While this agreement includes some improvements in comparison with the 2007 agreement, and includes adequate safeguards on data security and oversight, none of the main concerns expressed in the above mentioned opinions nor the conditions required by the European Parliament to provide its consent appear to have been met ([16]).

3. SPECIFIC REMARKS

3.1. The purpose should be clarified

8. Article 4(1) of the agreement states that the US processes PNR data for the purposes of preventing, detecting, investigating and prosecuting (a) terrorist offences and related crimes and (b) crimes that are punishable by a sentence of imprisonment of three years of more and that are transnational in nature. Some of these concepts are further defined.

9. Although these definitions are more precise than in the 2007 agreement, there are still some vague concepts and exceptions that could override the purpose limitation and undermine legal certainty. In particular:

— in Article 4(1)(a)(i), the wording 'conduct that (…) appears to be intended to intimidate or coerce' [or] 'influence the policy of a government' could also refer to activities which cannot be considered terrorist offences according to Council Framework Decision 2002/475/JHA ([17]); the notions 'appear to', 'intimidate' and 'influence' should be clarified to exclude this possibility,

— article 4(b) should contain a specific list of crimes; the reference to 'other crimes that are punishable by a sentence of imprisonment of three years of more' is not sufficient, as this threshold includes different crimes in the EU and the US and in the different EU Member States and US States.

([13]) EDPS Opinion of 25 March 2011 on the proposal for a Directive of the European Parliament and of the Council on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; EDPS Opinion of 15 July 2011 on the proposal for a Council Decision on the conclusion of an Agreement between the EU and Australia on the processing and transfer of PNR data by air carriers to the Australian Customs and Border Protection Service; EDPS Opinion of 19 October 2010 on the global approach to transfers of PNR data to third countries; and EDPS Opinion of 20 December 2007 on the proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes. All available on http://www.edps.europa.eu

([14]) WP29 Opinion 10/2011 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 7/2010 on European Commission's communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries; Opinion 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 and Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data. All available on http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm

([15]) FRA Opinion of 14 June 2011 on the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (available on http://fra.europa.eu/fraWebsite/attachments/FRA-PNR-Opinion-June2011.pdf) and EESC Opinion of 5 May 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 (available on http://www.eesc.europa.eu/?i=portal.en.soc-opinions.15579).

([16]) See footnote 5.

([17]) Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

— minor offences should be explicitly excluded from the purpose of the agreement,

— in Article 4(2), the concept of 'serious threat' should be defined and the use of PNR data where 'ordered by a court' should be limited to cases referred to in Article 4(1),

— similarly, in order to avoid the application of Article 4(3) to purposes such as border control, it should be specified that only the persons who are suspected of having taken part in any of the offences listed in Article 4(1) may be 'subject to closer questioning or examination.'

3.2. **The list of PNR data to be transferred should be narrowed**

10. Annex I of the agreement contains 19 types of data that will be sent to the US. Most of them also comprise different categories of data and are identical to the data fields in the 2007 agreement, which were already considered disproportionate by the EDPS and the Article 29 Working Party ([18]).

11. This refers in particular to the field 'General remarks including OSI ([19]), SSI ([20]) and SSR ([21]) information', which can reveal data related to religious beliefs (e.g. meal preferences) or to health (e.g. request for a wheelchair). Such sensitive data should be explicitly excluded from the list.

12. While assessing the proportionality of the list, it should also be taken into account that due to advanced transmission (Article 15(3) of the agreement), these categories will refer not only to actual passengers but also to those individuals who do not finally fly (e.g. due to cancellations).

13. In addition, the presence of open data fields could undermine legal certainty. Categories such as 'all available contact information', 'all baggage information' and 'general remarks' should be better defined.

14. Therefore, the list should be narrowed. In line with the Article 29 Working Party's opinion ([22]), we consider that data should be limited to the following information: PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items.

3.3. **The DHS should not process sensitive data**

15. Article 6 of the agreement states that the DHS shall automatically filter and 'mask out' sensitive data. However, sensitive data will be stored at least 30 days and might be used in specific cases (Article 6(4)). The EDPS would stress that even after being 'masked out', these data will still be 'sensitive' and relate to identifiable natural persons.

16. As already stated by the EDPS, the DHS should not process sensitive data related to EU citizens, even if they are 'masked out' upon reception. The EDPS recommends specifying in the text of the agreement that air carriers should not transfer sensitive data to the DHS.

([18]) See EDPS and WP29 opinions cited above.
([19]) Other Service related Information.
([20]) Special Services Information.
([21]) Special Service Requests.
([22]) See WP29 Opinion 4/2003, cited above.

3.4. **The retention period is excessive**

17. Article 8 states that PNR data will be retained for up to five years in an active database and then transferred to a dormant database and stored for up to 10 years. This maximum retention period of 15 years is clearly disproportionate, irrespective of whether the data are kept in 'active' or 'dormant' databases, as already underlined by the EDPS and the Article 29 Working Party.

18. Article 8(1) specifies that the data will be 'depersonalised and masked' six months after their reception by the DHS. However, both 'masked out' data and data stored in a 'dormant database' are personal data as long as they are not anonymised. The data should therefore be anonymised (irreversibly) or deleted immediately after analysis or after a maximum of six months.

3.5. **Use of the 'push' method and frequency of the transfers**

19. The EDPS welcomes Article 15(1), which states that data will be transferred using the 'push' method. However, Article 15(5) requires carriers to 'provide access' to PNR data in exceptional circumstances. In order to definitively preclude the use of the 'pull' system, and in view of the concerns recently once again underlined by the Article 29 Working Party ([23]), we strongly advise that the agreement expressly prohibits the possibility for US officials to separately access the data via a 'pull' system.

20. The number and periodicity of the transfers from air carriers to the DHS should be defined in the agreement. To enhance legal certainty, the conditions in which additional transfers would be allowed should also be more detailed.

3.6. **Data security**

21. The EDPS welcomes Article 5 of the agreement on data security and integrity and, in particular, the obligation to notify the affected individuals of a privacy incident. However, the following elements of the data breach notification should be clarified:

— the recipients of the notification: it should be specified which 'relevant European authorities' should be notified, and in any case, these should include national Data Protection Authorities — a competent US authority should also be notified,

— the threshold of the notification to these authorities: it should be defined what constitutes a 'significant privacy incident',

— the content of the notification to individuals and to authorities should be specified.

22. The EDPS supports the obligation to log or document all access and processing to PNR, as this will allow a verification of whether the DHS has made appropriate use of the PNR data and whether there has been any unauthorised access to the system.

3.7. **Supervision and enforcement**

23. The EDPS welcomes the fact that compliance with the privacy safeguards in the agreement will be subject to independent supervision and oversight by Department Privacy Officers such as the DHS Chief Privacy Officer, as stated in Article 14(1). However, in order to ensure an effective exercise of

([23]) See Letter of 19 January 2011 from the Article 29 Working Party to Commissioner Malmström regarding the EU PNR Agreements with the US, Canada and Australia.

data subjects' rights, the EDPS and the national Data Protection Authorities should work with the DHS on the procedures and modalities of exercise of these rights ([24]). The EDPS would welcome a reference to this cooperation in the agreement.

24. The EDPS strongly supports the right to redress 'regardless of nationality, country of origin, or place of residence' laid down in Article 14(1), second subparagraph. However, he regrets that Article 21 explicitly states that the agreement 'shall not create or confer, under US law, any right or benefit on any person'. Even if a right to 'judicial review' is granted in the US under the agreement, such right may not be equivalent to the right to effective judicial redress in the EU, in particular in the light of the restriction stated in Article 21.

3.8. **Onward national and international transfers**

25. Article 16 of the agreement prohibits the transfer of the data to domestic authorities that do not afford to PNR 'equivalent or comparable' safeguards to those set forth in this agreement. The EDPS welcomes this provision. The list of authorities that might receive PNR data should however be further specified. As regards international transfers, the agreement provides that they should only take place if the recipient's intended use is consistent with this agreement and adduces privacy safeguards 'comparable' to the ones provided in the agreement, except in emergency circumstances.

26. With regard to the wording 'comparable' or 'equivalent' used in the agreement, the EDPS would like to emphasise that no domestic or international onward transfers by the DHS should take place unless the recipient adduces safeguards that are not less stringent than the ones established 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, and no exceptions should be allowed. In addition, the EDPS recommends that data transfers to third countries should be subject to prior judicial authorisation.

27. Article 17(4) states 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 in cases where the DHS is aware of this situation. This condition should be deleted, as the DHS should always be aware of onward transfers to third countries.

3.9. **Form and review of the agreement**

28. 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.

29. Article 20(2) addresses coherence with the possible EU PNR scheme. The EDPS notes that consultations on the adjustment of this agreement shall in particular examine 'whether any future EU PNR system would apply less stringent data protection safeguards than those provided for in the present agreement'. In order to ensure consistency, any adjustment should also (and particularly) take account of stronger safeguards in any future PNR scheme.

30. The agreement should also be reviewed in view of the new data protection framework and of the possible conclusion of a general agreement between the EU and the US on the exchange of personal data in the framework of police and judicial cooperation in criminal matters. A new provision similar to Article 20(2) could be added stating that 'if and when a new data protection legal framework is adopted in the EU or a new agreement on the exchange of data between the EU and the US is concluded, the Parties shall consult each other to determine whether the present Agreement would

([24]) The Article 29 Working Party has for example already provided guidance on the provision of information to passengers (see WP29 Opinion 2/2007 of 15 February 2007 (revised and updated on 24 June 2008) on information to passengers about the transfer of PNR data to US authorities, available on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_en.pdf).

need to be adjusted accordingly. Such consultations shall in particular examine whether any future modification of the EU data protection legal framework or any future EU-US data protection agreement would apply more stringent data protection safeguards than those provided for in the present agreement'.

31. As regards the review of the agreement (Article 23), the EDPS considers that national Data Protection Authorities should be explicitly included in the review team. The review should also concentrate on assessment of the necessity and proportionality of the measures, on the effective exercise of data subjects' rights, and include the verification of the way in which data subjects' requests are being processed in practice, especially where no direct access is allowed. The frequency of the reviews should be specified.

4. **CONCLUSION**

32. The EDPS welcomes the safeguards on data security and oversight foreseen in the agreement and the improvements in comparison with the 2007 agreement. However, many concerns remain especially as regards coherence of the global approach to PNR, purpose limitation, the categories of data to be transferred to the DHS, the processing of sensitive data, the retention period, the exceptions to the 'push' method, the rights of data subjects and onward transfers.

33. These observations are without prejudice to the necessity and proportionality requirements for any legitimate PNR scheme and agreement providing for the bulk transfer of PNR data from the EU to third countries. As the European Parliament reaffirmed in its resolution of 5 May, 'necessity and proportionality are key principles without which the fight against terrorism will never be effective'.

Done at Brussels, 9 December 2011.

Peter HUSTINX

European Data Protection Supervisor