EDPS comments on the Proposals for Council Decisions on the conclusion and the signature of the 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

RESTRICTED

Introduction

The agreement between the EU and Australia on PNR data is a further step in the EU agenda, 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 recently adopted two Opinions on the "PNR package" of the Commission and the Proposal for a Directive on EU-PNR[1].

While the general approach which aims at harmonising data protection safeguards in the various PNR agreements with third countries is welcome, several objections remain. In particular two recurring problems are present.

First, a consistent remark reiterated in EDPS Opinions and in Opinions of the Article 29 Working Party[2] equally applies to the Australian PNR proposal: the necessity and proportionality of the PNR scheme have not been demonstrated. In particular, the EDPS has not found convincing elements in the Privacy Impact Assessment conducted by the Commission in the context of the Proposal for a Directive on EU-PNR. It is also questionable whether the agreements already in place, such as the EU-US agreement on PNR data, have proven to be necessary.

Second, the period of data retention is a problem, as discussed *infra*.

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, enforcement and oversight, as well as those relating to onward transfers. At the same time, we express concern, in addition to the necessity and proportionality of the scheme, 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

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

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 3 of the Proposals. The EDPS has insisted earlier on the importance of a strictly defined purpose limitation. We note however that -compared to the definitions of the Proposal for a Directive on EU-PNR (which should still have been further narrowed down, especially with regard to minor offences)- the present definitions are even wider.

  While in the EU-PNR Proposal definitions take into account the *consequences* of activities defined as "terrorist", such as concrete damages to persons or governments (death, attacks upon the physical integrity, destruction to a transport system, an infrastructure facility, etc), the present Proposal is less specific and more *purpose* oriented when it refers to intimidating persons, governments, or seriously destabilising fundamental political or economic structures.

  We consider that more precision is needed in relation to the notions of "intimidating, compelling and coercing", as well as the "fundamental *political*, *constitutional*, *economic*, or (especially) *social* structures of a country or an international organisation". This would prevent the application of the PNR scheme in cases which it should in any event not target, such as legitimate activities in a social, cultural or political context.

  The possibility to process data in other exceptional cases raises additional questions, especially as it extends to "threat to health". We consider that such an extension of purpose is disproportionate, especially as it is not clear whether the threat to health is limited to cases of vital interest.

  We also note that the list of PNR data annexed to the Proposals exceeds what has been considered as proportionate by Data Protection Authorities in Article 29 Working Party Opinions[3]. This list should be reduced. In particular the field "General remarks" should be deleted, as this can contain irrelevant -and potentially sensitive- data.

- Sensitive data

  We welcome the exclusion of the processing of sensitive data, as stated in Article 8 of the Proposals. However, the drafting of this provision leads to think that even though sensitive data purportedly may not be processed, they may well be *sent* in the first place by airlines, and deleted by public authorities in a second stage, both none the less acts of *processing*. We consider that airlines should filter out sensitive data at the source of the processing.

- Data security

  The Proposals include in Article 9 a comprehensive provision on data security and integrity, which is welcome. We support in particular the obligation to report security breaches to the Office of the Australian Information Commissioner. With regard to the

[3] Opinion of 23 June 2003 on the Level of Protection ensured in the United States for the Transfer of Passengers' Data, WP78.

further sending of information to the European Commission, further explanations would be needed. We consider that Data Protection Authorities would in any case be relevant recipients of this kind of information and should be included in the Proposal.

- 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 also strongly supported. We consider the role of the Office of the Australian Information Commissioner as an important guarantee as far as redress possibilities and exercise of data subjects' rights are concerned.

- Automated individual decisions

  According to Article 15, interpreted *a contrario*, an automated decision which "significantly affects or produces an adverse legal effect on a passenger" is allowed as long as it is not taken solely on the basis of the automated processing of data. The notion of "significantly affects" is questionable in our view. To avoid any flexible interpretation of this provision, we recommend deleting these words and ensuring that no automated decision at all is allowed which produces an adverse effect on an individual.

- Retention of data

  We consider the length of the data retention period as foreseen in Article 16 as one of the major difficulties in the proposal. A period of retention of five and a half years, including three years without any masking of data, is disproportionate, especially if this retention period is compared with the previous Australian PNR scheme which did not foresee the storage of data except on a case by case basis[4].

  In line with the position advocated in the EDPS Opinion on the Proposal for a Directive for an EU-PNR, we consider that the complete (i.e. irreversible) anonymization of all data should take place, if not immediately after analysis, after 30 days as a maximum.

- Onward transfers

  The guarantees provided in Articles 18 and 19 are welcome, especially as they provide for a list of recipients of data transferred within Australia, for a transfer on a case-by-case basis and an assessment of the necessity of the transfer in each case. As an additional safeguard, we suggest limiting transfers to authorities "whose main task is to combat terrorism or transnational crime", rather than those authorities whose functions are "directly related to preventing (these) crimes".

[4] See in this respect the positive opinion of the Article 29 Working Party: Opinion 1/2004 of 16 January 2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines, WP85. The opinion takes into account the fact that "Customs applies a general policy of non retention for these data. For those 0.05% to 0.1% of passengers who are referred to Customs for further evaluation, the airline PNR data are temporarily retained, but not stored, pending resolution of the border evaluation. After resolution, their PNR data are erased from the PC of the Customs PAU officer concerned and are not entered into Australian databases".

The fact that transfers to third countries are subordinated to the condition that they provide the "same" safeguards as the original agreement is supported. We suggest in addition that these transfers are subject to a prior judicial authorisation.

Finally, the Proposals foresee that when data of a resident of an EU Member State are transferred to a third country, the Member State concerned should be informed where the Australian Customs and Border Protection Service is aware of this situation. We consider that further details should be included explaining the purpose for such a transmission to a Member State. Would such a transmission of information have an impact on the data subject, additional justification and safeguards should be included.

- Transfers by airlines

According to Article 21.3, transfers of PNR data to authorities can take place more than five times in exceptional circumstances, in case of specific threat. To enhance legal certainty, the conditions of such additional transfers should be more detailed.

- Review of the agreement

We consider that the conditions for the review should be more detailed on several aspects. The frequency of reviews after the initial review should be specified. Moreover, Data Protection Authorities should be explicitly included in the review team, and not simply in a conditional way.

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.