

Opinion of the European Data Protection Supervisor

on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

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 the request for an opinion in accordance with 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 its Article 41,²

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

I. Consultation of the EDPS

1. On 21 September 2010, the Commission adopted a Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries.³ The Communication was sent to the EDPS for consultation on the same day.

¹ OJ L 281, 23.11.1995, p. 31

² OJ L 8, 12.01.2001, p. 1

³ COM (2010) 492 final.

2. The EDPS welcomes the fact that he was consulted by the Commission. Already before the adoption of the Communication, the EDPS was given the possibility to give informal comments. Some of these comments have been taken into account in the final version of the document, while other points still raise data protection concerns.

2. *The proposal in its context*

3. The global approach to PNR issues presented by the Commission in its communication aims at providing a coherent framework for the transfer of PNR data to third countries. Beyond the need for legal certainty developed in the Communication, this harmonised approach has also been strongly supported by the European Parliament which is entrusted in the new institutional framework with the power to ratify PNR agreements with third countries⁴.
4. The Communication is complemented by Recommendations for negotiations of PNR agreements with specific third countries. These Recommendations are restricted and are not analysed in this opinion. However, the relation between the general Communication and the Recommendations is commented upon in chapter II.
5. In addition to the global approach to transfers of PNR data to third countries, the Commission is also preparing a revised approach to PNR for the EU. Earlier, a proposal for such an EU framework was intensively discussed in Council, under the former third pillar before the entry of the Lisbon Treaty.⁵ These discussions did not lead to a consensus on a number of essential elements of the PNR-system, such as for instance the use of the data base created under such a system. The Stockholm Programme then urged the Commission to come with a new proposal, but it did not address the essential elements of such a proposal. A draft Directive for an EU PNR scheme is expected in the beginning of 2011.
6. The present opinion focuses on the Communication of the Commission. Its first part analyses the Communication in the context of current developments in the area of data protection, the second part addresses the legitimacy of the PNR scheme and the third part focuses on more specific data protection issues in the Communication.

⁴ Agreements have been signed with:

- the United States: 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) (2007 PNR Agreement) (OJ L 204, 4.8.2007, p. 18).
- Canada: 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).
- Australia: Agreement between the European Union and Australia on the processing and transfer of European Union sourced passenger name record (PNR) data by air carriers to the Australian customs service (OJ L213 of 08/08/2008, p.49-57).

⁵ On 6 November 2007, the Commission adopted a Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (COM(2007) 654 final). The EDPS presented his opinion on this proposal on 20 December 2007 (OJ 2008, C 110/1).

II. ANALYSIS OF THE PROPOSAL

1. General observations

7. The EDPS welcomes the horizontal approach of the Communication, in line with the recent requests of the European 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.
8. The EDPS nevertheless questions the general timing of the different initiatives directly or indirectly related to the processing of PNR data.
9. While the Communication mentions international agreements on PNR schemes *and* the initiative for an EU PNR, the proposed standards in the Communication relate *only* to international agreements. The EU framework will be discussed and developed at a later stage.
10. A more logical and opportune agenda would in the view of the EDPS have included an in-depth reflection on a possible EU scheme including data protection safeguards compliant with the EU legal framework, and on this basis, developing an approach for agreements with third countries.
11. The EDPS also emphasises the ongoing work in relation with an EU-US general agreement on data sharing for law enforcement⁶, the purpose of which is to establish a set of principles guaranteeing a high level of protection for personal data as a condition to the exchange of such data with the United States. The outcome of the EU-US negotiations should be a reference for further bilateral agreements concluded by the EU and by its Member States, including the PNR agreement between the EU and the US.
12. Another element to take into consideration in this context is the general reflection on the EU data protection framework which is now conducted by the Commission, with a view to a Communication before the end of 2010 to be followed by a proposal for a new regulatory framework in the course of 2011⁷. This review process takes place in the "post-Lisbon" framework, which has a direct impact on the horizontal application of data protection principles to the former pillars of the EU, including police and judicial cooperation in criminal matters.
13. To ensure consistency, the EU should agree on its internal instruments and on the basis of these internal instruments it should negotiate agreements with third countries. The global agenda should therefore concentrate first on the general EU data protection framework, then on the possible need for an EU PNR scheme, and finally on the

⁶ See notably the Consultation launched by the Commission in January 2010 on the future European Union (EU) - United States of America (US) international agreement on personal data protection and information sharing for law enforcement purposes and the contributions of the Article 29 Working party and the EDPS, to be found at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0005_en.htm

⁷ The Commission has launched a process of review of the current legal framework which started with a high level conference in May 2009. It has been followed by a public consultation until the end of 2009 and by several stakeholder consultation meetings in July 2010. The contribution of the Article 29 Working Party, in which the EDPS has taken an active part, is available at the following link: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#general_issues

conditions for exchanges with third countries, based on the updated EU framework. At this stage the safeguards foreseen in a future EU-US agreement should also be taken into account while establishing conditions for transfers of PNR data to third countries.

14. The EDPS is aware of the fact that, for different procedural and political reasons, this ideal order is not being followed in practice. He considers nevertheless that the logic behind these different steps should be kept in mind by the different actors involved in the Commission, the Council and the Parliament. As developments, notably on the EU framework and the EU-US negotiations, are progressing in parallel, due account should be taken of this need for consistency and for a harmonised view on data protection safeguards within the EU and in the context of transfers. To be more concrete, this would imply notably:

- taking into account the results of the impact assessment on the EU PNR before finalising any PNR negotiations with third countries
- ensuring that lessons are learned from the reviews of current PNR arrangements;
- and, as far as negotiations with the United States are concerned, linking PNR negotiations with the negotiations on the general agreement on data sharing for law enforcement. This is the only way to ensure consistent safeguards in both agreements.

15. Finally, the EDPS raises the question of the link between the Communication and the guidelines drafted by the Commission. The issue concerns the extent to which precise safeguards and conditions should be specified 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, the EDPS considers 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.

2. *Legitimacy of the scheme*

16. The EDPS as well as the Article 29 Working Party have already insisted in a number of opinions⁸ on the need for a clear justification of 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 supported by concrete evidence, and it should then be evaluated and balanced with the degree of intrusion in the private life of individuals in order to ensure a proportionate and least invasive outcome. The fact that recent technological developments currently render wide access and analysis possible, as stated at the end of point 2.2 of the Communication, is not in itself a justification for the development of a system aimed at the screening of all travellers. In other words: the availability of means should not justify the end.

⁸ Opinion of the EDPS of 20 December 2007 on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, OJ C 110, 01.05.2008, p. 1. 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

17. As developed below, the EDPS considers that the bulk transfer of data about innocent people for risk assessment purposes raises serious proportionality issues. The EDPS questions in particular the proactive use of PNR data. While "re-active" use of data does not raise major concerns, *as far as it is part of an investigation of a crime already committed*, real time and proactive use lead to a more critical assessment.
18. According to the wording of the Communication, even in the "real time context", PNR data will be "use(d) in order to prevent a crime, survey or arrest persons before a crime has been committed", based on "predetermined fact-based risk indicators"⁹. The main idea to take measures with regard to persons before a crime has been committed on the basis of risk indicators, is in the view of the EDPS a proactive measure, the use of which in a law enforcement context is traditionally strictly defined and limited.
19. Besides, neither the notion of risk indicators, nor the notion of "risk assessment" is sufficiently developed, and the latter could easily be confused with the notion of "profiling". This similarity is even strengthened by the alleged objective which is to establish "fact based travel and behavioural patterns". The EDPS questions the link between the original facts, and the patterns deduced from these facts. The process aims at imposing on an individual a risk assessment - and possibly coercive measures - based on facts which are not related to this individual. As already stated in his previous opinion on a proposal for an EU-PNR, the main concern of the EDPS relates to the fact that "decisions on individuals will be taken on the basis of patterns and criteria established using the data of passengers in general. Thus decisions on one individual might be taken, using as a reference (at least partially), patterns derived from the data of *other* individuals. It is thus in relation to an abstract context that decisions will be taken, which can greatly affect data subjects. It is extremely difficult for individuals to defend themselves against such decisions"¹⁰.
20. The use of such techniques on a wide scale involving the screening of all passengers therefore raises serious questions of compliance with fundamental privacy and data protection principles, including those laid down in Article 8 ECHR, Articles 7 and 8 of the Charter and Article 16 TFEU.
21. 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 being conducted in the framework of the EU PNR project. The agenda should be set in order to allow a careful consideration of the results of this impact assessment in the drafting of global requirements for PNR schemes.

3. *Content of the proposed standards*

22. Without prejudice to the preceding fundamental comments on the legitimacy of PNR schemes, the EDPS welcomes the extensive list of standards, visibly inspired by EU data protection principles, which in several aspects should strengthen the protection foreseen in specific agreements. The added value and shortcomings identified in these standards are discussed hereafter.

⁹ Page 4 of the Communication, chapter 2.1.

¹⁰ Opinion of 20 December 2007 on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, OJ C 110, 01.05.2008, p. 4.

Adequacy and binding character of any agreement

23. From the wording of the Communication, the EDPS understands that the assessment of adequacy can be based on the general data protection framework of the recipient country or be contextual, depending on legally binding commitments in an international agreement governing the processing of personal data. Considering the decisive role of international agreements in relation to adequacy assessments, the EDPS emphasizes the need to clearly establish the binding character of agreements for all parties concerned, and he believes this should be complemented by an explicit indication that the agreements shall ensure *directly enforceable rights* to data subjects. The EDPS considers that these elements constitute an essential aspect of the adequacy assessment.

Scope and purpose

24. 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. The EDPS questions this wording which could lead to consider that future agreements would not be based precisely on these definitions but would be inspired by them. It is essential for reasons of legal certainty that terrorism and serious transnational crimes are precisely defined and that EU instruments referred to in the Communication are identified. Besides, the EDPS recalls that before different types of crimes are included in the PNR scheme, they must as a pre-condition pass a necessity and proportionality test.

25. The second point seems to refer more to the scope (the nature of data collected) than to the purpose principle. The EDPS notes that the Communication does not include a list of data which could be subject to transfers, as it leaves to each specific agreement the determination of categories of data to be exchanged. To avoid divergences and inclusion of disproportionate categories of data in some agreements with third countries, the EDPS considers that a common and exhaustive list of categories of data should be added to the standards, in line with the purpose of the exchange of data. He refers to the opinions of the Article 29 Working Party in this respect, which indicate the categories of data which would be admissible and those considered as excessive in relation to the fundamental rights of data subjects¹¹. Categories of data to be excluded are notably those which can be regarded as sensitive data - and which are protected by Article 8 of Directive 95/46, SSR/SSI data (Special Service Request/Information), OSI (Other Service-Related Information) data, open or free-text fields (such as the "General Remarks" where data of a sensitive nature can appear), and the information concerning frequent-flyers and "behavioural data".

Sensitive data

26. The Communication indicates that sensitive data shall not be used unless in exceptional circumstances. The EDPS deplors this exception. He considers that the conditions of the exception are too broad and do not bring any guarantees: use on a case by case basis of the data is only presented as an example; besides, the purpose

¹¹ 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

limitation should be a general principle applicable to any processing of PNR data, not only a guarantee applying to sensitive data. The EDPS considers that 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. He therefore calls for a complete exclusion of the processing of sensitive data, as a principle.

Data security

27. The general obligation on security developed in the Communication is considered as satisfactory. The EDPS considers nevertheless that it could be complemented by an obligation of mutual information in case of security breach: recipients would be responsible for informing their counterparts in case data they received have been subject to unlawful disclosure. This will contribute to enhanced responsibility towards a secure processing of the data.

Enforcement

28. The EDPS supports 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, he understands 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 notably an indirect right of access should be clearly mentioned in the standards.

Onward transfers

29. The EDPS is satisfied with the restriction of onward transfers on a case by case basis, be it to other government authorities or to third countries. He considers that, in addition to this principle, the purpose limitation applicable to transfers to third countries should also apply to transfers within the third country to other government authorities. This should prevent any further use or cross-checking of the PNR data with information processed for different purposes. The EDPS is concerned in particular with the risk of cross-checking with information originating from other databases such as ESTA with regard to the United States. He notes that the recent US decision to require a fee for ESTA results in the collection of credit card information of travellers. The EDPS calls for a clear limitation to prevent inappropriate matching of information beyond the scope of the PNR agreement.

Data retention

30. The period of retention of data is not subject to effective harmonisation. The EDPS considers that, as a principle, PNR data should be deleted if the controls made at the occasion of the transmission of data have not triggered any enforcement action. Would the national context justify the need for a limited period of retention, the EDPS considers that a maximum period of retention should be established in the standards. Besides, the principle of limiting access rights of officials in time should be reinforced and the gradual anonymisation of data should be considered as an obligation and not as an example.

Modalities of transmission

31. The EDPS supports the exclusive use of the "push" system to transmit PNR data. He calls for concrete guarantees ensuring that "push" is effectively the only system used in practice. Experience and inspections conducted by data protection authorities have indeed shown that despite the obligations of agreements already in force, in particular with regard to the "US PNR ", a residual "pull" is still effective and that in parallel to "push", US authorities have a wider access to PNR data through Computer Reservation Systems. Legal and technical measures should be taken to prevent any bypassing of the "push" system.
32. The frequency of transmissions by airlines ("reasonable") should be defined, and a maximum number of transmissions should be established. Existing schemes providing for the most privacy compliant provisions should be the benchmark for such exercise.

Overarching concepts

33. The EDPS also calls for more precision with regard to essential elements of the implementation of PNR agreements. The duration of agreements ("fixed", "appropriate") and their review ("periodical") should be further defined in a horizontal perspective. The periodicity of joint reviews, in particular, could be specified, as well as the obligation to conduct a first review within a specific deadline after the entering into force of the agreements: a maximum of three years could be mentioned.

III. CONCLUSION

34. The EDPS welcomes the horizontal approach presented by the Commission in its communication. This is an essential step in the direction of a comprehensive framework for the exchange of PNR data. Some major concerns however mitigate this general appreciation.
35. PNR schemes presented in the Communication do not *per se* meet the necessity and proportionality tests as developed in this opinion and in previous opinions of the EDPS and the Article 29 Working Party. To be admissible, the conditions for collection and processing of personal data should be considerably restricted. The EDPS is in particular concerned about the use of PNR schemes for risk assessment or profiling.
36. The development of PNR standards should take into account the general data protection framework and related legal developments within the EU, as well as the negotiation of data exchange agreements at a more general level, especially with the United States. It should be ensured that a future agreement on PNR with the United States respects the general agreement on data protection with the US. Agreements on PNR with other third countries should also be consistent with this approach.
37. It is essential that any agreement with third countries takes into account the new data protection requirements as they are being developed in the post-Lisbon institutional framework.

38. The EDPS also calls for more precision in the global approach with regard to the minimal safeguards applicable to all agreements: stricter conditions should apply especially with regard to the processing of sensitive data, the purpose limitation principle, the conditions of onward transfers and the retention of data.
39. The EDPS finally insists on the fact that any agreement should provide for directly enforceable rights to data subjects. The effectiveness of enforcement procedures, by data subjects as well as by supervisory authorities, is an essential condition for the assessment of the adequacy of any agreement.

Done in Brussels, 19 October 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor