I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes

(2008/C 110/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

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 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 ([2]), and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 13 November 2007 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

Consultation of the EDPS

1. The draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation No 45/2001/EC (hereinafter 'the proposal').

2. The proposal concerns the processing of PNR data within the EU and is closely related to other schemes of collection and use of passengers' data, in particular the EU-US agreement of July 2007. These schemes are of great interest to the EDPS, who already had the opportunity to send some preliminary comments on the Commission's questionnaire on the intended EU PNR system, sent in December 2006 to relevant stakeholders ([3]). The EDPS welcomes the consultation of the Commission. According to the EDPS, the present opinion should be mentioned in the preamble of the Council Decision.

The proposal in its context

3. The proposal intends to harmonise Member States' provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime.

4. Arrangements for transmission of PNR data for comparable purposes have been concluded by the European Union with the USA, as well as with Canada. A first agreement concluded with the USA in May 2004 was replaced

([1]) OJ L 281, 23.11.1995, p. 31.
([2]) OJ L 8, 12.1.2001, p. 1.

([3]) Including Member States, Data Protection Authorities and airlines associations. This questionnaire had been prepared in view of the preparation of an impact assessment by the European Commission on the present proposal.

by a new agreement in July 2007 ([1]). A similar agreement was concluded with Canada in July 2005 ([2]). In addition, negotiations are due to start between the EU and Australia for an agreement on the exchange of PNR data, and South Korea is also requiring PNR data from flights to its territory, without any plan for negotiation at European level at this stage.

5. Within the EU, the proposal comes as an addition to Council Directive 2004/82/EC ([3]) on the obligation of carriers to communicate passengers' data known as API data, in order to combat illegal immigration and improve border control. This directive should have been transposed in national law of Member States not later than 5 September 2006. Implementation is however not ensured yet in all Member States.

6. Contrary to Advanced Passenger Information (API) data that are supposed to help identifying individuals, PNR data mentioned in the proposal would contribute to carrying out risk assessments of persons, obtaining intelligence and making associations between known and unknown people.

7. The proposal includes the following main elements:

— It provides for the making available by air carriers of PNR data to the competent authorities of Member States, for the purpose of preventing and combating terrorist offences and organised crime.

— It foresees the designation of a Passenger Information Unit (PIU) in principle in each Member State, responsible for collecting the PNR data from air carriers (or designated intermediaries) and for carrying out a risk assessment of passengers.

— Information assessed accordingly will be transmitted to competent authorities in each Member State. This information will be exchanged with other Member States on a case by case basis and for the purpose indicated above.

— Transfer to countries outside the European Union is subject to additional conditions.

— Data will be retained for thirteen years, eight of which in a dormant database.

— The processing is to be governed by the (draft) Council Framework decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (hereafter the 'data protection framework decision') ([4]).

— A Committee with representatives of Member States will assist the Commission with regard to protocol and encryption issues, as well as with regard to criteria and practice for risk assessment.

— A review of the decision is to take place within three years after its entry into force.

Focus of the opinion

8. The proposal on which the EDPS is consulted is a further step in a movement towards a routine collection of data of individuals who are in principle not suspected of any crime. As mentioned above, this evolution is taking place at international and European level.

9. The EDPS notes that also the Article 29 Working Party and the Working Party on Police and Justice have presented a joint opinion on the proposal ([5]). The EDPS supports that opinion. The present opinion emphasises and develops a number of additional points.

10. While the opinion of the EDPS will analyse all relevant aspects of the proposal, it will concentrate on four main issues.

— The first of these issues is the legitimacy of the intended measures. The question of the purpose, necessity and proportionality of the proposal will be assessed against the criteria of Article 8 of the Charter of Fundamental Rights of the European Union.

— The opinion will also analyse the question of the law applicable to the proposed processing operation. In particular, the scope of application of the data protection framework decision in relation to the application of first pillar data protection legislation deserves specific attention. The consequence of the applicable data protection regime with regard to the exercise of data subject's rights will also be questioned.

([1]) 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).

([2]) 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).

([3]) Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

([4]) The latest draft of this proposal is available on Council register as document number 16397/07.

([5]) Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, adopted by the Article 29 Working Party on 5 December 2007 and by the Working Party on Police and Justice on 18 December 2007, WP 145, WPPJ 01/07.

— The opinion will then focus on the quality of recipients of data at national level. In particular, the quality of PIUs, of intermediaries and of competent authorities designated to perform risk assessment and analyse passenger data raises specific concerns as no precision is given in the proposal in this respect.

— The fourth issue relates to the conditions of transfer of data to third countries. It is not clear what conditions will apply to such transfers where different sets of rules exist: the conditions of transfer under the present proposal, together with those of the data protection framework decision, and the existing international agreements (with the USA and Canada).

11. Other substantive points will be identified in a last part, including positive steps in terms of data protection but also additional sources of concern in the proposal.

II. LEGITIMACY OF THE PROPOSED MEASURES

12. In order to analyse the legitimacy of the proposed measures in accordance with fundamental data protection principles, and notably Article 8 of the European Charter of Fundamental Rights and Articles 5 to 8 of Council of Europe Convention No 108 ([1]), it is necessary to identify clearly the purpose of the intended processing of personal data, to assess its necessity and its proportionality. It should be ensured that no other means is available, that would be less invasive, to reach the envisaged purpose.

Identification of purpose

13. The wording of the proposal and its impact assessment indicate that the objective is not simply to identify known terrorists or known criminals involved in organised crime, by comparing their names with those included in lists managed by law enforcement authorities. The purpose is to gather intelligence with regard to terrorism or organised crime, and more precisely 'to carry out risk assessment of persons, obtain intelligence and make association between known and unknown people' ([2]). The purpose stated in Article 3(5) of the proposal is, in the same line and firstly, 'to identify persons who are *or may be* involved in a terrorist or organised crime offence, *as well as their associates*.'

14. This is the reason invoked to explain that API data are not sufficient to reach the alleged purpose. Indeed, as already mentioned, while API data are supposed to help identifying individuals, PNR data do not have an identification purpose, but the details of the PNR would contribute to carrying out risk assessments of the persons, obtaining intelligence and making associations between known and unknown people.

15. The purpose of the measures envisaged does not only cover the catching of *known* persons but also the locating of persons that *may* fall within the criteria of the proposal.

In order to identify these persons, risk analysis and identification of patterns are at the core of the project. Recital 9 of the proposal states explicitly that data must be kept 'for a sufficiently long period as to fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour'.

16. The purpose is thus described in two layers: the first layer consists of the global objective to fight against terrorism and organised crime, while the second layer includes the means and measures inherent to the achievement of this objective. While the purpose of fighting terrorism and organised crime appears to be clear enough and legitimate, the means used to reach this purpose leave room for discussion.

Establishing patterns and risk assessment

17. The proposal gives no indication on the way patterns will be established and risk assessment will be performed. The impact assessment gives the following precision as to the way PNR data will be used: to run the data of passengers 'against a combination of characteristics and behavioural patterns, aimed at creating a risk-assessment. When a passenger fits within a certain risk-assessment, then he could be identified as a high-risk passenger' ([3]).

18. Suspected persons could be selected according to concrete elements of suspicion included in their PNR data (e.g. contact with a suspicious travel agency, reference of a stolen credit card), as well as on the basis of 'patterns' or an abstract profile. Different standard profiles could indeed be constituted on the basis of travel patterns, for 'normal passengers' or 'suspicious passengers'. These profiles would enable investigating further those passengers who do not fall within the 'normal passenger category', all the more so if their profile is associated with other suspicious elements such as a stolen credit card.

19. Although it cannot be assumed that passengers would be targeted according to their religion or other sensitive data, it appears nevertheless that they would be subject to investigation on the basis of a mix of *in concreto* and *in abstracto* information, *including* standard patterns and abstract profiles.

([1]) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.
([2]) Explanatory Memorandum of the proposal, Chapter I.
([3]) Impact assessment, Chapter 2.1, 'Description of the problem'.

20. One could discuss whether this type of investigation would qualify as profiling. Profiling would consist of a 'computer method making use of data mining on a data warehouse, enabling or intended to enable the classification, with some probability — and thus with some margin of error — of an individual in a specific category in order to take individual decisions towards that person' ([1]).

21. The EDPS is aware that there are ongoing discussions on the definition of profiling. Whether or not it is officially recognised that the proposal aims at *profiling* passengers, the main point at stake is not about definitions. It is about the impact on individuals.

22. 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.

23. In addition, the risk assessment is to be performed in absence of uniform standards of identification of suspects. The EDPS seriously questions the legal certainty of the whole filtering process, considering that the criteria against which every passenger will be scanned are so poorly defined.

24. The EDPS recalls the jurisprudence of the European Court of Human Rights, according to which domestic law must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to file information on their private life and make use of it. The information 'should be accessible to the person concerned and foreseeable as to its effects'. A rule is 'foreseeable' 'if it is formulated with sufficient precision to enable any individual — if need be with appropriate advice — to regulate his conduct' ([2]).

25. To conclude, it is notably because of these types of risks, that the present proposal needs careful consideration. While the general purpose to fight against terrorism and organised crime is in itself clear and legitimate, the core of the processing to be put in place does not appear to be sufficiently circumscribed and justified. The EDPS therefore urges the EU-legislator to clearly address this issue, before adoption of the Framework Decision.

Necessity

26. The intrusive character of the measures is evident, as shown above. On the other hand, their utility is far from being demonstrated.

27. The impact assessment on the proposal concentrates on the best way to establish an EU PNR, more than on the necessity of such PNR. Reference is made in the assessment ([3]) to PNR systems in place in other countries, namely the USA and the United Kingdom. One can however deplore the lack of precise facts and figures related to those systems. 'Numerous arrests' are reported with regard to 'various crimes' in the UK semaphore system, without precision as to the link with terrorism or organised crime. No details are given with regard to the US programme, except that 'the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes'.

28. Not only is there a lack of precise information *in the proposal* on the concrete results of such PNR systems, but reports published *by other agencies*, e.g. the GAO in the United States, do not confirm at this stage the efficiency of the measures ([4]).

([1]) This definition comes from a recent study on profiling of the Council of Europe: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, November 2007 (*not published yet*). See also the definition by Lee Bygrave: 'Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components: (i) profile generation — the process of inferring a profile; (ii) profile application — the process of treating persons/entities in light of this profile '. L. A. BYGRAVE, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24 http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru v. Romania, No 28341/95, §§ 50, 52 and 55. See also Amann v. Switzerland, No 27798/95, §§ 50 *et s.*

([3]) Chapter 2.1., 'Description of the problem'.

([4]) See e.g. the report of the United States Government Accountability Office to congressional requesters, May 2007, 'Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain' http://www.gao.gov/new.items/d07346.pdf

29. The EDPS considers that techniques consisting of assessing the risk presented by individuals using data mining tools and behavioural patterns need to be further assessed, and their utility be clearly established in the framework of the fight against terrorism, before they are used on such a wide scale.

Proportionality

30. In order to appreciate the balance between the intrusion in the privacy of the individual and the necessity of the measure ([1]), the following elements are taken into account:

— The measures apply to all passengers, be they under investigation or not by law enforcement authorities. It constitutes proactive research, on an unprecedented scale.

— Decisions on individuals can be based on abstract profiles, thus including a significant margin of error.

— The nature of the measures to be taken against the individual relate to law enforcement: the consequences in terms of exclusion or coercion are therefore much more intrusive than in other contexts, like credit card fraud or marketing.

31. Compliance with the proportionality principle implies not only that the proposed measure is effective, but also that the purpose envisaged by the proposal can not be reached using the less privacy invasive tools. The effectiveness of the intended measures has not been demonstrated. The existence of alternatives must be carefully assessed before additional/new measures are put in place to process personal information. According to the EDPS, such comprehensive assessment has not taken place.

32. The EDPS wishes to recall the other large scale systems monitoring the movements of individuals within or at the borders of the EU, whether in operation or about to be implemented, including in particular the Visa Information System ([2]) and the Schengen Information System ([3]). While these instruments do not have as a main goal the fight against terrorism or organised crime, they are or will be to some extent accessible to law enforcement authorities for the broader scope of the fight against crime ([4]).

33. Another example concerns the availability of personal data included in national police data bases — especially with regard to biometric information — in the framework of the Prüm Treaty signed in May 2005, that is being extended to all Member states of the European Union ([5]).

34. These different instruments all have in common that they enable a global monitoring of movements of individuals, even if from different perspectives. The way in which they can already contribute to the fight against specific forms of crimes, including terrorism, should be subject to in-depth and comprehensive analysis, before deciding to establish a new form of systematic scanning of all persons leaving or entering the EU by plane. The EDPS recommends that the Commission conducts such an analysis, as a necessary step in the legislative procedure.

Conclusion

35. In the light of the foregoing, the EDPS concludes as follows on the legitimacy of the proposed measures. Building upon different data bases without a global view on the concrete results and shortcomings:

— Is contrary to a rational legislative policy in which new instruments must not be adopted before those existing have been fully implemented and proved to be insufficient ([6]).

— Might otherwise lead to a move towards a total surveillance society.

36. The fight against terrorism can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection. However, to be valid, the necessity of the intrusion must be supported by clear and

([1]) According to article 9 of Convention 108, 'derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
1. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
2. protecting the data subject or the rights and freedoms of others.'

([2]) Council decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (OJ L 213, 15.6.2004, p. 5). Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2005) 0835 final; Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, COM(2005) 0600 final.

([3]) See in particular Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007).

([4]) See on this issue: Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005) 600 final) (OJ C 97, 25.4.2006, p. 6).

([5]) See the EDPS Opinions on the Prüm Decisions: Opinion of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ C 169, 21.7.2007, p. 2), and Opinion of 19 December 2007 on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, available at: http://www.edps.europa.eu

([6]) This point has been made several times by the EDPS, most recently in its opinion of 25 July 2007 on the Implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1).

undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of extensive intrusion in the privacy of individuals, as foreseen in the proposal.

37. It can only be noted that such elements of justification are missing in the proposal and that the necessity and proportionality tests are not fulfilled.

38. The EDPS insists on the essential character of the necessity and proportionality tests developed above. They represent a *condicio sine qua non* to the entry into force of the present proposal. Any further comment of the EDPS in the present opinion must be taken in the light of this preliminary condition.

III. APPLICABLE LAW — EXERCISE OF DATA SUBJECT'S RIGHTS

Applicable law

39. The analysis below will concentrate on three points:

— a description of the different steps of the processing foreseen in the proposal, with a view to identifying the law applicable at each stage,

— the limitations of the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters in terms of scope and in terms of rights of the data subject,

— a more general analysis of the extent to which a third pillar instrument can apply to private actors processing data in a first pillar framework.

Applicable law at different steps of the processing

40. Article 11 of the proposal states that 'Member States shall ensure that the Council Framework Decision on the Protection of Personal data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (…) is applicable to the processing of personal data under this Framework Decision.'

41. However, in spite of this provision it is not clear to what extent the data protection framework decision — an instrument under the third pillar of the EU Treaty — will be applicable to data processed by airlines, collected by PIUs, and further used by other competent authorities.

42. The first step in the processing of personal data foreseen by the proposal is processing by the airlines, which are obliged to make PNR data available — using in principle a push system — to national PIUs. It seems from the wording of the proposal and the impact assessment [1] that data could also be transmitted in bulk by airlines to intermediaries. Airlines are primarily active in a commercial environment, subject to national data protection legislation implementing Directive 95/46/EC [2]. Questions on the applicable law will arise when data collected are used for law enforcement purposes [3].

43. Data would then be filtered by an intermediary (to be formatted and to exclude PNR data not included in the list of data required by the proposal) or sent directly to PIUs. Intermediaries could also be actors from the private sector, as is the case for SITA, operating in that sense in the framework of the PNR Agreement with Canada.

44. When it comes to PIUs, responsible for the risk assessment of the whole amount of data, it is not clear who will be responsible for the processing. Customs and border authorities might be involved, and not necessarily law enforcement authorities.

45. The subsequent transmission of filtered data to 'competent' authorities would probably happen in a law enforcement context. The proposal states that 'competent authorities shall only include authorities responsible for the prevention or combating of terrorist offences and organised crime'.

46. While moving forward through the steps of the processing, the actors involved and the purpose followed have a closer link with police and judicial cooperation in criminal matters. The proposal does not explicitly mention, however, when precisely the data protection framework decision will apply. The wording would even lead to think that it applies to the whole processing, and even to the airlines [4]. However, the framework decision on the protection of personal data includes in itself some limitations.

---

[1] Article 6.3 of the proposal and Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

[2] 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 (OJ L 281, 23.11.1995, p. 31).

[3] See in this respect the consequences of the PNR judgement. Judgement of the Court of 30 May 2006, European Parliament v Council (C-317/04) and Commission (C-318/04), Joined cases C-317/04 and C-318/04, ECR [2006], Point 56.

[4] Article 11 of the proposal. See also recital 10 of the preamble: 'The Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters (…) should be applicable to all the data processed in accordance with this Framework Decision. The rights of the data subjects in relation to such processing, such as the right to information, the right of access, the right of rectification, erasure and blocking, as well as the rights to compensation and judicial remedies should be those provided under that framework decision'.

47. In this context, the EDPS fundamentally questions the fact whether Title VI of the EU-Treaty can serve as a legal basis for legal obligations on a routine basis and for law enforcement purposes upon private sector actors. Additionally, the question is relevant whether Title VI of the EU-Treaty can serve as a legal basis for legal obligations on public authorities which are in principle outside the framework of law enforcement cooperation. These questions will be elaborated further on in this opinion.

Limitations of the data protection framework decision

48. The text of the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters contains at least two limitations which are relevant in terms of scope.

49. In the first place, the scope of the data protection framework decision is well defined in the framework decision itself: it applies 'only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' ([1]).

50. In the second place, the data protection framework decision is not supposed to apply to data processed purely at domestic level, but is limited to data exchanged between Member States and further transfer to third countries ([2]).

51. The data protection framework decision also includes some drawbacks compared to Directive 95/46/EC, in particular a wide exception to the purpose limitation principle. With regard to this purpose principle, the proposal clearly limits the purpose of the processing to the fight against terrorism and organised crime. However, the data protection framework decision allows processing for wider purposes. In such a case, the *lex specialis* (the proposal) should prevail over the *lex generalis* (the data protection framework decision) ([3]). This should be made explicit in the text of the proposal.

52. For this reason, the EDPS recommends adding the following provision to the proposal: 'Personal data transmitted by airlines according to this Framework Decision may not be processed for purposes other than the fight against terrorism and organised crime. The exceptions foreseen with regard to the purpose principle in the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters do not apply'.

53. As a conclusion, the EDPS notes a serious lack of legal certainty with regard to the data protection regime applicable to the different actors involved in the project, and in particular to airlines and other first pillar actors: be it the rules of the proposal, the rules of the data protection framework decision or the national legislation implementing Directive 95/46/EC. The legislator should make clear at what moment of the processing precisely these different rules will apply.

Conditions of application of first and third pillar rules

54. The EDPS fundamentally questions the fact that a third pillar instrument creates legal obligations on a routine basis and for law enforcement purposes upon private or public sector actors which are in principle outside the framework of law enforcement cooperation.

55. A comparison could be made here with two other cases where the private sector was involved in the retention or transfer of data in a perspective of law enforcement:

— *The US-PNR case where a systematic transfer of PNR data by airlines to law enforcement authorities was foreseen*. The judgement of the Court of Justice in the PNR case excluded Community competence to conclude the PNR agreement. One of the justifications was that the transfer of PNR data to the US CBP constituted processing operations concerning public security and the activities of the State in areas of criminal law ([4]). In this case, the processing operation was a transfer to the CBP *in a systematic fashion*, which makes a difference with the following case:

— *The general retention of data by electronic communication operators*. With regard to the Community competence to establish such a retention period, a difference can be made with the US-PNR case, considering that Directive 2006/24/EC ([5]) only foresees an obligation of retention, with data remaining under the control of the operators. No systematic transfer of data to law enforcement authorities is envisaged. It can be concluded that, as far as the data remain under the control of the service providers, those providers also remain responsible for the respect of personal data protection obligations vis-à-vis the data subject.

([1]) Recital 5(a), version of 11 December 2007 of the data protection framework decision.
([2]) Article 1.
([3]) With regard to this point, the text of Article 27b of the latest draft of the Framework decision on data protection in the third pillar should be carefully considered and discussed.
([4]) Judgement of the Court of 30 May 2006, European Parliament v Council (C-317/04) and Commission (C-318/04), Joined cases C-317/04 and C-318/04, ECR [2006], Point 56.
([5]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

56. In the present EU PNR proposal, airlines have to make available in a systematic way the PNR data of all passengers. However, these data are not transferred directly in bulk to law enforcement authorities: they can be sent to an intermediary and they are assessed by a third party, the statute of which remains unclear, before selected information is sent to competent authorities.

57. The main part of the processing happens in a grey zone, having material links with the first as well as with the third pillar. As it will be developed in Chapter IV, the quality of actors processing the data is not clear. Airlines are obviously no enforcement authorities, and intermediaries could be actors of the private sector. Even with regard to PIUs which would be public authorities, it must be stressed that not every public authority has the quality and the competences to perform law enforcement tasks on a routine basis.

58. Traditionally, a clear separation has existed between law enforcement and private sector activities, where law enforcement tasks are performed by specifically dedicated authorities, in particular police forces, and private actors are solicited on a case by case basis to communicate personal data to these enforcement authorities. There is now a trend to impose cooperation for law enforcement purposes on private actors on a systematic basis, which raises the question which data protection framework (first or third pillar) applies to the conditions of this cooperation: should the rules be based on the quality of the data controller (private sector) or on the purpose followed (law enforcement)?

59. The EDPS has already recalled the risk of a legal loophole between the first and third pillar activities ([1]). It is indeed far from clear whether activities by private companies, in some way connected with enforcement of criminal law, are covered by the field of action of the European Union legislator under the Articles 30, 31 and 34 TEU.

60. If the general (first pillar) framework would not apply, a service provider should have to make difficult distinctions within his data bases. Under the current regime, it is clear that the data controller has to respect the same data protection vis-à-vis the data subjects irrespectively of the purposes that justify the retention of data. An outcome in which processing by service providers for different purposes would be subject to different frameworks for data protection should therefore be avoided.

([1]) See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also the Annual Report 2006, p. 47.

Exercise of data subject's rights

61. The different legal regimes that would apply at national level would have a major impact primarily on the exercise of his/her rights by the data subject.

62. It is stated in the preamble of the proposal that 'information, access, rectification, erasure and blocking, compensation and judicial remedies are to be provided under the data protection framework decision'. However, this statement does not answer the question of who the controller in charge of answering data subjects' requests is.

63. While information on the processing could be communicated by airlines, the issue is more complex when it comes to access or rectification of data. These rights are indeed restricted under the data protection framework decision. As stated above, it is doubtful that a service provider such as an airline could be obliged to give differentiated access and rectification rights to the data it holds, depending on the purpose (commercial or law enforcement) followed. One might argue that these rights are to be exercised before the PIU or the otherwise designated competent authorities. The proposal however gives no further indication in this respect, and as already mentioned, it is not clear either that these authorities (at least PIUs) will be law enforcement authorities normally entrusted with restricted (possibly indirect) access procedures.

64. The individual also risks being confronted with different recipients of data, as far as PIUs are concerned: the data are indeed transmitted to the PIU of the country of departure/arrival of flights, but also possibly to PIUs of other Member States on a case by case basis. Moreover, it is possible that several member States may establish or designate one single and common PIU. The data subject might in that case have to exercise redress before an authority of another Member State. Here again, it is not clear whether the national data protection rules will apply (these are supposed to be harmonised within the EU), or if specific law enforcement legislation will have to be taken into account (given the lack of comprehensive harmonisation in the third pillar at national level).

65. The question is the same with regard to access to data processed by intermediaries, the statute of which is unclear, and which could also be common to airlines in different countries of the EU.

66. The EDPS deplores the uncertainty that remains with regard to the exercise of these fundamental rights of the data subject. He stresses the fact that this situation is mostly due to the fact that actors who do not have law enforcement as a principal task are entrusted with such responsibilities.

Conclusion

67. The EDPS considers that the proposal should make clear what legal regime is applicable at which stage of the processing, and specify vis-à-vis which actor or authority access and redress shall be exercised. The EDPS recalls that according to Article 30.1. b) TEU, provisions on data protection should be appropriate and cover the full range of processing operations established by the proposal. A simple reference to the data protection framework decision is not sufficient, given the limited scope of that framework decision and the restriction of rights it contains. As far as law enforcement authorities are involved, the rules of the data protection framework decision should at least apply to the whole processing foreseen in the proposal, in order to guarantee the coherence of the application of data protection principles.

IV. QUALITY OF RECIPIENTS

68. The EDPS notes that the proposal does not provide for any specification with regard to the quality of the recipients of personal data collected by airlines, be it for intermediaries, Passenger Information Units, or competent authorities. It must be stressed that the quality of the recipient is in direct relation with the type of data protection guarantees applying to that recipient. The difference between guarantees provided in particular by first and third pillar rules has already been mentioned. It is essential that the applicable regime be clear for all actors involved, including national governments, law enforcement agencies, the data protection authorities, as well as data controllers and data subjects involved.

Intermediaries

69. No indication is given in the proposal with regard to the quality of intermediaries ([1]). The role of intermediaries as controllers or processors is not specified either. From experience, it seems that a private sector entity, be it a Computer Reservation System or another entity, could perfectly be entrusted with the task of gathering PNR data directly from the airlines to redirect them to PIUs. It is indeed the way data are processed under the PNR Agreement with Canada. SITA ([2]) is the company responsible for the processing of the information. The role of the intermediary is decisive, as it could be responsible for the filtering out/reformatting of data that are transmitted in bulk by airlines ([3]). Even if intermediaries are obliged to cancel the processed information once it has been transferred to PIUs, the processing in itself is highly sensitive: a consequence of the intervention of intermediaries is the creation of an additional database including massive amounts of data, and even, according to the proposal, sensitive data (intermediaries being obliged then to delete those sensitive data). For these reasons, the EDPS recommends that no intermediaries should be involved in the processing of passenger data, unless their quality and tasks are strictly specified.

Passenger information units

70. PIUs have a decisive role in identifying persons that are or may be involved or associated with terrorism or organised crime. According to the proposal, they will be responsible for creating risk indicators and providing intelligence on travel patterns ([4]). Where the risk assessment is based on standardised travel patterns and not on material evidence linked with a concrete case, the analysis can be considered as constituting proactive investigation. The EDPS stresses that this kind of processing is in principle strictly regulated in Member State legislation (if not prohibited), and it is the task of specific public authorities the functioning of which is also strictly regulated.

71. PIUs are therefore entrusted with very sensitive processing of information, without the proposal giving any detail on their quality and the conditions in which they would exercise this competence. Although it is likely that this task will be performed by a governmental body, possibly customs or border control, the proposal does not explicitly prevent Member States to entrust intelligence agencies or even any kind of processor with its performance. The EDPS underlines the fact that the transparency and guarantees applying to intelligence agencies are not always identical to those applicable to traditional law enforcement authorities. Details on the quality of PIUs are decisive, as this will have direct consequences on the applicable legal framework and the conditions of supervision. The EDPS considers that the proposal must include an additional provision detailing the specificities of PIUs.

([1]) Article 6 of the proposal.

([2]) SITA was created in 1949 by 11 member airlines. Value-added solutions are provided to air transport industry through the commercial company SITA INC (Information, Networking Computing) and network services through SITA SC on a co-operative basis.

([3]) Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

([4]) Article 3 of the proposal.

Competent authorities

72. It appears from Article 4 of the proposal that any authority responsible for the prevention or combating of terrorist offences and organised crime can receive the data. While the purpose is clearly defined, the quality of the authority is missing. The proposal does not foresee any limitation of recipients to law enforcement authorities.

As mentioned above with regard to PIUs, it is decisive that the sensitive information at stake be processed in an environment with a clear legal framework. This is much more the case, e.g., for law enforcement authorities than for intelligence agencies. Considering the data mining elements and the proactive research included in the proposal, it cannot be excluded that such intelligence agencies be involved in the processing of the data, without exclusion of any other type of authorities.

Conclusion

73. As a general comment, the EDPS notes that the enforcement of an EU PNR system is rendered even more difficult considering that law enforcement authorities have different competences depending on the national law of the Member States, including or not intelligence, tax, immigration or police. This is however a supplementary reason to recommend that the proposal be much more precise with regard to the quality of the mentioned actors and the guarantees to control the performance of their tasks. Additional provisions should be integrated in the proposal, to specify strictly the competences and the legal obligations of intermediaries, PIUs and other competent authorities.

V. CONDITIONS OF TRANSFER TO THIRD COUNTRIES

74. The proposal provides for some safeguards in relation to the transfer of PNR data to third countries ([1]). In particular, it foresees explicitly the application of the data protection framework decision to data transfers, it provides for a specific purpose limitation and it states the need for consent of the Member State in case of onward transfer. The transfer should also comply with national legislation of the Member State concerned, as well as any applicable international agreement.

75. Many questions remain however, in particular with regard to the quality of consent, the conditions of application of the data protection framework decision and the question of 'reciprocity' in the transmission of data to third countries.

([1]) Article 8 of the proposal.

Quality of consent

76. The Member State of origin must give express consent for onward transfer of data from a third country to another third country. The proposal does not specify under what conditions and by whom this consent will be given, and whether national DPAs should be involved in the decision. The EDPS considers that the way consent will be given should at least be in conformity with national laws stating conditions of transfer of personal data to third countries.

77. Besides, consent of a Member State should not prevail over the principle according to which an adequate level of protection must be foreseen by the recipient country for the intended processing. These conditions should be cumulative, as they are in the data protection framework decision (Article 14). The EDPS therefore suggests adding a point (c) to paragraph 1 of Article 8 that would read 'and (c) the third State ensures an adequate level of protection for the intended data processing.' The EDPS recalls in this respect that mechanisms ensuring common standards and coordinated decisions with regard to adequacy must be put in place ([2]).

Application of the data protection framework decision

78. The proposal refers to the conditions and safeguards contained in the data protection framework decision while also specifying explicitly some conditions, in particular the above mentioned consent of the Member State concerned, and a limitation of the purpose to preventing and fighting terrorist offences and organised crime.

79. The data protection framework decision itself provides for conditions to the transfer of personal data to third countries, namely with regard to the purpose limitation, the quality of recipients, the consent of Member State, and the adequacy principle. However, it also foresees derogations to these conditions of transfer: legitimate prevailing interests, especially important public interests, can be a sufficient basis for transfer even if the conditions listed above are not fulfilled.

80. As already mentioned in Chapter III of this opinion, the EDPS considers that it must be stated clearly in the text of the proposal that the more precise guarantees of the proposal prevail over the general conditions — and exceptions — of the data protection framework decision, where it applies.

([2]) Opinion of the EDPS of 26 June 2007 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, points 27 to 30 (OJ C 139, 23.6.2007, p. 1).

Reciprocity

81. The proposal addresses the issue of possible 'retaliation requests' of countries that might ask the EU for PNR data for flights from the EU to their territory. Where the EU requests data from databases of airlines of such third countries, because they operate a flight to or from the EU, such third country could ask the same from airlines based in the EU, including data from citizens of the EU. Although the Commission considers this eventuality as 'very remote', it allows for it. The proposal refers in this regard to the fact that the agreement with the US and with Canada foresee such reciprocal treatment 'which may be enforced automatically' ([1]). The EDPS questions the significance of such an automatic reciprocity and the application of safeguards to such transfers, notably taking into account the existence of an adequate level of protection of the country concerned.

82. A distinction should be made between third countries which have already concluded an agreement with the EU, and those countries which do not have such agreement.

Countries having no agreement with the EU

83. The EDPS notes that reciprocity might lead to transfer personal data to countries where no guarantees can be provided in terms of democratic standards and adequate level of data protection.

84. The impact assessment gives further elements with regard to the conditions of transfer of data to third countries: the advantage of the EU-PNR system, where data are filtered by PIUs, is emphasised. Only selected data of suspected individuals (and not bulk data) would be transferred to the competent authorities of Member States and presumably to third countries as well ([2]). The EDPS recommends clarifying this point in the text of the proposal. A simple statement in the impact assessment does not provide for the necessary protection.

85. While the selection of data would contribute to minimise the impact on the privacy of passengers, it must be recalled that data protection principles go far beyond data minimisation, and include principles such as necessity, transparency and exercise of data subject rights, all principles to be taken into account when determining whether a third country provides for an adequate level of protection.

Countries having a bilateral agreement with the EU

86. The impact assessment indicates that such processing will provide the EU with the ability 'to insist on certain standards and to ensure consistency in such bilateral agreements with third countries. It will also provide for the possibility of requesting reciprocal treatment from third countries with which the EU has an agreement, something that is not possible today' ([3]).

87. From these observations arises the question of the impact of the proposal on the existing agreements with Canada and the USA. The conditions of access to data in these agreements are indeed much broader, as they are not subject to a similar selection before being transferred to those third countries.

88. The impact assessment indicates that 'in cases in which the EU has an international agreement with a third country for the exchange/transmission of PNR data to such third country, such agreements shall be duly taken into account. The carriers should send the PNR data to the Passengers Information Units according to the normal practice under the current measure. The PIU which receives such data shall transmit them to the competent authority of the third country with which such an agreement exists' ([4]).

89. While on the one hand, the proposal seems to aim at a transfer of *only selected* data to any competent authority, be it within the EU or outside, on the other hand, the impact assessment, the preamble of the proposal (recital 21) and Article 11 itself recall that existing agreements should be duly taken into account. This might lead to the conclusion that filtering may only be a valid measure for agreements to be concluded in the future. It could be foreseen in this perspective that bulk access will still be the rule for access e.g. by US authorities to PNR data, in conformity with the provisions of the EU-US agreement, but that in parallel and on a case by case basis, a transfer of data to the US could occur, relating to specific data identified by PIUs, including but not limited to data concerning flights to the US.

90. The EDPS regrets the lack of clarity on this decisive point of the proposal. He considers of the utmost importance that the conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection. Besides, for reasons of legal certainty, precisions with regard to the guarantees applying to the transfer of data should be included in the proposal itself and not only in the impact assessment, as it is the case now.

([1]) Explanatory Memorandum of the proposal, Chapter 2.
([2]) Impact assessment, Chapter 5.2., 'Protection of privacy'.
([3]) Impact assessment, Chapter 5.2., 'Relations with third countries'.
([4]) Impact assessment, Annex A, 'Bodies receiving data from the Passenger Information Units'.

VI. OTHER SUBSTANTIVE POINTS

Automated processing

91. The EDPS notes that the proposal explicitly excludes that enforcement actions be taken by the Passenger Information Units and the competent authorities of the Member Sates only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation ([1]).

92. Such precision is welcome as it limits the risks of arbitrary measures against individuals. The EDPS however notes that its scope is limited to *enforcement actions* by PIUs or competent authorities. It does not exclude, in its present wording, the automated filtering of individuals according to standard profiles, nor does it prevent the automated constitution of lists of suspected persons and the taking of measures such as extended surveillance, as long as these measures are not considered as enforcement actions.

93. The EDPS considers that the notion of *enforcement actions* is too vague, and that, as a principle, *no decision* should be taken with regard to individuals *only* by reason of the automated processing of their data ([2]). The EDPS recommends modifying the text accordingly.

Quality of data

94. The proposal gives in Article 5.2 an important precision as it makes clear that no obligation is put on airlines to collect or retain additional data to those collected for the initial commercial purpose.

95. Several aspects of the processing of these data still deserve further comment:

— The data to be made available, as listed in Annex 1 of the proposal, are very extensive, and the list is similar to the list of data available to US authorities in the EU-US agreement. The quality of some of the data requested has already been questioned at several occasions by Data Protection Authorities, and especially by the Article 29 Working Party ([3]).

— It seems from the wording of the impact assessment ([4]) and Article 6.3 of the proposal that data could also be transmitted in bulk by airlines to intermediaries. In a first stage, data transmitted to a third party would not even be limited in compliance with the PNR data listed in Annex 1 of the proposal.

— With regard to the processing of sensitive data, even if these data might be filtered out at the stage of intermediaries, the question still remains whether the transfer of the open field by airlines is strictly necessary.

The EDPS supports the points made in the WP29-opinion in this respect.

Method of transfer of PNR data

96. Air carriers established outside the EU are required to *push* data to PIUs or intermediaries as long as they possess the technical architecture to do it. If this is not the case they will have to permit the extraction of data through the *pull* method.

97. Allowing for different methods of communication of data depending on the airlines concerned will only raise more difficulties with regard to the control of the compliance of transfer of PNR data with data protection rules. This risks as well to distort competition between EU and non-EU airlines.

98. The EDPS recalls that the push method, allowing airlines to keep control on the quality of data transferred and the circumstances of transfers, is the only admissible method with regard to the proportionality of the processing. Besides, it must consist of an effective push, that is, the data should not be sent in bulk to an intermediary but filtered at the very first step of the processing. It is not admissible that non necessary data — and data not included in Annex 1 of the proposal — be sent to a third party, even if those data are to be deleted immediately by this third party.

Data retention

99. Article 9 of the proposal foresees a 5 years retention period of PNR data, with an additional 8 years period where data are to be kept in a 'dormant' database that will be accessible in restricted conditions.

([1]) Recital 20 and Article 3.3 and 3.5 of the proposal.

([2]) See in this respect Article 15.1 of Directive 95/46/EC. The Directive prohibits such automated decisions in cases where the individual would be affected by the decision. With regard to the context of the proposal, decisions in a law enforcement framework are likely to affect severely the data subjects in any case. Also the fact of being subject to secondary checks can affect the data subject, especially if these actions are taken repeatedly.

([3]) See in particular Opinion No 5/2007 of 17 August 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, WP 138.

([4]) Impact assessment, Annex A, 'Method of transmission of the data by the carriers'.

100. The EDPS questions the difference between the two types of data bases: it is questionable whether the dormant database constitutes a real archive, with different methods of storage and retrieval of data. Indeed, most of the conditions put to the access to the dormant database consist of security requirements that could be applicable to the 'five years retention database' as well.

101. The total duration of storage — that is 13 years — is in any case excessive. It is justified in the impact assessment by the need to develop risk indicators and establish patterns of travel and behaviour ([1]), the efficiency of which deserves further demonstration. While it is obvious that data can be retained as long as necessary in a specific case as far as an investigation is ongoing, no justification can support the retention of data of all passengers in total absence of suspicion for 13 years.

102. The EDPS further notes that this retention period is not supported by the answers of Member States to the questionnaire of the Commission, according to which the average duration of storage required would be 3,5 years ([2]).

103. Moreover, the period of 13 years is comparable to the retention period of 15 years in the most recent agreement with the United States. The EDPS has always understood that this long retention period was only agreed upon because of strong pressure by the US Government to have a much longer period than 3.5 years, not because it was in any stage defended by the Council or the Commission. There is no reason to transpose such a compromise — that only has been justified as a necessary result of negotiations — to a legal instrument within the EU itself.

Role of the Committee of Member States

104. The Committee of Member States established under Article 14 of the proposal will be competent with regard to security issues including protocol and encryption of PNR data, but also with regard to guidance for common general criteria, methods and practices related to risk assessment.

105. Apart from these indications, the proposal does not include any element or criteria with regard to the concrete conditions and framework of the risk assessment process. The impact assessment mentions that the criteria will ultimately depend on intelligence held by each Member State, which is constantly evolving. The risk assessment is to be performed in absence of uniform standards of identification of suspects. The extent to which the Committee of Member States will be able to play a role in this regard thus appears questionable.

Security

106. The proposal details a series of security measures ([3]) to be taken by PIUs, intermediaries and other competent authorities in order to protect the data. Considering the importance of the data base and the sensitivity of the processing, the EDPS considers that in addition to the measures envisaged, the entity processing the data should also be obliged to officially notify any security breach.

107. The EDPS is aware of the project to establish such a notification procedure in the sector of electronic communications at European level. He advises to include such safeguard in the present proposal, and refers in this respect to the security breach system put in place in the United States with regard to state agencies ([4]). Security incidents can indeed happen in any field of activity, and in the private as well as the public sector, as the recent loss of a whole citizens' database by the British administration has shown ([5]). Large scale databases such as the one envisaged in the proposal would be first on a priority list to benefit from such an alert system.

Review and Sunset Clause

108. The EDPS notes that a review is to take place within three years of the entry into force of the framework decision, on the basis of a report prepared by the Commission. He acknowledges the fact that this review, based on information provided by Member States, will give specific attention to data protection safeguards, and include the implementation of the 'push' method, the data retention and the quality of the risk assessment. Such review should, to be comprehensive, include the results of an analysis of the statistical data produced on the basis of the processing of PNR information. These statistics should, in addition to the elements mentioned in Article 18 of the proposal, include statistical details on the identification of high risk persons, such as the criteria for such identification and the concrete results of any law enforcement action resulting of the identification.

([1]) Impact assessment, Annex A, 'Data retention period'.
([2]) Impact assessment, annex B.
([3]) Article 12 of the proposal.
([4]) See in particular the works of the American 'Identity Theft Task Force':
http://www.idtheft.gov/
([5]) See the link to the British HM Revenue and Customs website:
http://www.hmrc.gov.uk/childbenefit/update-faqs.htm
See also:
http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. The EDPS has already insisted in this opinion on the absence of concrete elements to establish the necessity of the system proposed. He considers however that, should the framework decision enter into force, it should as a minimum be complemented by a sunset clause. At the end of the three years period, the Framework Decision should be repealed in case no element would come to support its continuation.

Impact on other legal instruments

110. In its final provisions the proposal puts a condition to the further application of already existing bilateral or multilateral agreements or arrangements. Those instruments can only be applied as far as they are compatible with the objectives of the proposed framework decision.

111. The EDPS questions the scope of this provision. As already mentioned in Chapter V under Reciprocity, it is not clear what the impact of this provision will be on the content of agreements with third countries, such as the agreement with the US. In a different perspective, it is not clear either whether the provision could have an impact on the conditions of application of instruments with a broader scope, such as Council of Europe Convention No 108. Although this might appear unlikely in view of the difference of institutional context and actors involved, any risk of misinterpretation should be avoided and the proposal should make clear that it does not have any impact on instruments with a broader scope, notably those having as object the protection of fundamental rights.

VII. **CONCLUSION**

112. The EDPS stresses the major impact in terms of data protection of the present proposal. He has concentrated his analysis on four fundamental issues raised by the proposal, and insists on the fact that the issues raised need to be addressed in a comprehensive manner. Under the present circumstances, the proposal is not in conformity with fundamental rights, notably Article 8 of the Charter of the Fundamental Rights of the Union, and should not be adopted.

113. Should the comments above be complied with, especially the legitimacy test, some drafting proposals have been made in the present opinion that should be taken into account by the legislator. Reference is made in particular to points 67, 73, 77, 80, 90, 93, 106, 109 and 111 of the opinion.

Legitimacy of the proposed measures

114. While the general purpose to fight against terrorism and organised crime is in itself clear and legitimate, the core of the processing to be put in place is not sufficiently circumscribed and justified.

115. The EDPS considers that techniques consisting of assessing the risk presented by individuals using data mining tools and behavioural patterns need to be further assessed, and their utility be clearly established in the framework of the fight against terrorism, before they are used on such a wide scale.

116. Building upon different data bases without a global view on the concrete results and shortcomings:

— Is contrary to a rational legislative policy in which new instruments must not be adopted before existing instruments have been fully implemented and proved to be insufficient.

— Might otherwise lead to a move towards a total surveillance society.

117. The fight against terrorism can certainly be a legitimate ground to apply exceptions to the fundamental rights to privacy and data protection. However, to be valid, the necessity of the intrusion must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of extensive intrusion in the privacy of individuals, as foreseen in the proposal.

118. These elements of justification are missing in the proposal and the necessity and proportionality tests are not fulfilled.

119. The EDPS insists on the essential character of the necessity and proportionality tests developed above. They represent a *condicio sine qua non* to the entry into force of the proposal.

Applicable legal framework

120. The EDPS notes a serious lack of legal certainty as to the regime applicable to the different actors involved in the project, and in particular to airlines and other first pillar actors: be it the rules of the proposal, the rules of the data protection framework decision or the national legislation implementing Directive 95/46/EC. The legislator should make clear at what stages of the processing these different rules will apply.

121. The present trend to impose cooperation for law enforcement purposes on private actors on a systematic basis raises the question which data protection framework (first or third pillar) applies to the conditions of this cooperation: it is not clear whether the rules should be based on the quality of the data controller (private sector) or on the purpose followed (law enforcement).

122. The EDPS has already stressed the risk of a legal loophole between the first and third pillar activities ([1]). It is indeed far from clear whether activities by private companies, in some way connected with enforcement of criminal law, are covered by the field of action of the European Union legislator under the Articles 30, 31 and 34 TEU.

123. An outcome in which processing by service providers for different purposes would be subject to different frameworks for data protection should be avoided, especially considering the difficulties this would create in terms of exercise of rights by data subjects.

Quality of recipients

124. The proposal should provide for a specification with regard to the quality of the recipients of personal data collected by airlines, be it for intermediaries, Passenger Information Units, or competent authorities.

125. The quality of the recipient, that could in some cases be private sector actors, is in direct relation with the type of data protection guarantees applying to that recipient. It is essential that the applicable regime be clear for all actors involved, including the legislator, the data protection authorities, as well as data controllers and data subjects involved.

Transfer of data to third countries

126. The EDPS stresses the need to ensure that an adequate level of protection is provided in the recipient country. He also questions the significance of the 'reciprocity' principle mentioned in the proposal, and its application to countries already bound by an agreement with the EU, like Canada or the US. He considers it to be of the utmost importance that the conditions of transfer of PNR data to third countries be coherent and subject to a harmonised level of protection.

Other substantive points

127. The EDPS also draws the attention of the legislator to specific aspects of the proposal that need more precision or a better taking into account of data protection principle. This is the case in particular with regard the following aspects:

— the conditions in which automated decisions can be taken should be restricted,

— the quantity of data processed should be reduced,

— the method of transfer of data should solely rely on *push*,

— the data retention period is considered as excessive and not justified,

— the role of the committee of Member States could be more precise with regard to its guidance on 'risk assessment',

— the security measures should include a 'security breach notification' procedure,

— the review of the decision should include a sunset clause,

— the proposal should make clear that it does not have any impact on instruments with a broader scope having namely as object the protection of fundamental rights.

Final observations

128. The EDPS notes that the present proposal is made at a moment when the institutional context of the European Union is about to change fundamentally. The consequences of the Lisbon Treaty in terms of decision making will be fundamental, especially with regard to the role of the Parliament.

129. Considering the unprecedented impact of the proposal in terms of fundamental rights, the EDPS advises not to adopt it under the present Treaty Framework, but to ensure it follows the co-decision procedure foreseen by the new Treaty. This would strengthen the legal grounds on which the decisive measures envisaged in the proposal would be taken.

([1]) See the Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1). See also Annual Report 2006, p. 47.