Article 29 Data Protection Working Party
Working Party on Police and Justice

02422/07/EN
Art 29 WP ref: WP 145
WPPJ ref: 01/07

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 on 5 December 2007 by the Art. 29 Working Party

Adopted on 18 December 2007 by the Working Party on Police and Justice

Executive summary

This opinion aims to analyse the impact on fundamental rights and freedoms, in particular passengers' rights to privacy, of the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes presented by the European Commission on 6 November 2007.

The proposal is closely modelled on the EU-US PNR agreement signed in July 2007 and many features of the present draft are similar to that agreement. The privacy concerns raised by the Art. 29 Working Party on that PNR agreement therefore remain valid for a couple of points expressed in this opinion. The opinion also takes into account the findings of the Art. 29 Working Party's opinion 9/2006 of 27 September 2006 on Directive 2004/82/EC of the Council as that Directive also foresees the transfer of passenger by air carriers to government authorities.

The EU data protection authorities stress again that they have always supported the fight against international terrorism and organised crime. This fight is necessary and legitimate and personal data, and in particular some passenger data, might be valuable in assessing risks and preventing and combating terrorism and organised crime.
However, in the case of a European PNR regime the limitation of fundamental rights and freedoms has to be well justified and has to strike the right balance between demands for the protection of public security and the restriction of privacy rights.

The present draft foresees the collection of a vast amount of personal data of all passengers flying into or out of the EU regardless of whether they are under suspicion or innocent travellers. These data will then be stored for possible later use for a period of 13 years to allow for profiling. The proposal comes in addition to the fingerprinting of all citizens when applying for their passports as well as the retention of all telecommunications traffic data in the EU[1].

The current proposal must be considered a further milestone towards a European surveillance society in the name of fighting terrorism and organised crime.

The EU data protection authorities consider that the proposal as currently drafted is not only disproportionate but may violate fundamental principles of recognised data protection standards as enshrined in Art. 8 of the European Convention on Human Rights and Convention 108 of the Council of Europe. The applicability of the "Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Co-operation in Criminal Matters" as regards the rights of the data subject which the proposal refers to must be called into question, as that Framework Decision governs only the transfer of personal data between EU Member States' law enforcement agencies and not the transfer of data by air carriers to Passenger Information Units in the EU.

[1] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385 , 29/12/2004 P. 1.
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
- they have not been fully implemented in all member states yet.

The data protection related issues of this proposal can be characterised as follows.

1 The proposal does not justify a pressing need for the collection of data other than API data
2 The amount of personal data to be transferred by air carriers is excessive
3 The filtering of sensitive data should be done by the data controller
4 The 'push' method should apply to all air carriers
5 The data retention period is disproportionate
6 The data protection regime is completely unsatisfactory: the rights of the data subjects and the obligations of the controllers are nowhere specified
7 The great deal of discretion left to Member States might result in varying interpretations of the Framework Decision.
8 The data protection regime of onward transfers to third countries is unclear

The EU data protection authorities call on the Council to take into account the findings and recommendations of this opinion when debating the present proposal prior to its adoption. An open and frank debate with all stakeholders, i.e. the airline industry, the reservation systems, the data protection community, the European Parliament and national parliaments is indispensable if a balanced approach is to be reached.

An EU PNR regime must not lead to general surveillance of all travellers.

Opinion of the EU data protection authorities
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

I General remarks

On 6 November 2007 the Commission brought forward its proposal on a future Council Framework Decision on the use of passenger name record (PNR) for law enforcement purposes.
The independent EU data protection authorities and the European Data Protection Supervisor consider it necessary to carefully analyse this proposal as it will have far reaching consequences not only for travellers on their way into and out of the EU, but also for air carriers, reservations systems and law enforcement agencies.

In the past the Article 29 Working Party has had several opportunities to express its views on the use of passenger data for law enforcement purposes, in particular during the negotiations with the US and Canada on respective PNR agreements. It furthermore issued a detailed opinion (WP 127) in September 2006 on the obligation of air carriers to communicate advance passenger data which will be referred to repeatedly in this opinion due to the fact that the content of the draft proposal and Directive 2004/82/EC are closely related.

In addition, the Article 29 Working Party actively promoted the resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes, adopted during the 29th International Conference of Data Protection and Privacy Commissioners in Montreal, Canada, of 26-28 September 2007.

In preparing the proposal, the European Commission consulted several relevant stakeholders such as the air carriers. In January 2007 the Article 29 Working Party was also given the opportunity, by means of a questionnaire, to express its views and concerns. Some of the concerns specified in the answers have been addressed in the present proposal. Other concerns, however, mentioned in the replies and identified in this opinion still need to be addressed and require further attention in the future.

The EU data protection authorities (EU DPAs) stress that in the fight against terrorism and related crime, respect for fundamental rights and freedom of individuals including the right to privacy and data protection must be ensured and is not negotiable. Any limitation of such rights and freedoms must be well justified and has to strike the right balance between demands for the protection of public safety and other public interests such as the privacy rights of individuals.

The EU DPAs also want to underline the fact that although the use and storage of passenger data is intended for law enforcement purposes which is a third pillar matter, the air carriers collect such data initially for their own business purposes, which is purely a first pillar matter.

Furthermore it has to be mentioned that the EU Data Protection Commissioners are the supervisory authorities of the air carriers and the future Passenger Information Units and will be in charge of supervising the implementation of the Framework Decision.

This opinion will carefully analyse the level of data protection of this proposal in light of the fact that it will affect millions of travellers annually and that the proposal might seriously encroach into the privacy rights of all passengers concerned. When the EU DPAs comment on the level of data protection of the current proposal, they will take into account recognised data protection standards as enshrined in Art. 8 of the European Convention on Human Rights (ECHR), in Directive 95/46/EC[2] and in Convention 108 of the Council of Europe,[3] as well as the opinions adopted previously by the Article 29 Working Party on similar issues[4].

The EU DPAs also note that the profiling of **all** passengers envisaged by the current proposal might raise constitutional concerns in some Member States.

These recognised standards have to be applied to the proposal as to any other regulation which affects the privacy of citizens. The provisions of the proposal should, therefore, show that they are:

- demonstrably necessary to address a specific problem;
- demonstrably likely to address the problem;
- proportionate to the security benefit;
- demonstrably less privacy invasive than alternative options; and
- should be regularly reviewed to ensure the measures are still proportionate.

Furthermore any proposal should provide for data minimisation; explicit limits on use, disclosure and retention appropriate to the purpose of the scheme; data accuracy; rights of access and correction and independent review.

II The proposal

Introduction

The proposal for the Council Framework Decision on the use of passenger name record (PNR) for law enforcement purposes requires all air carriers flying into and out of the EU to transfer the listed data elements as far as they are contained in their reservation system(s) to Passenger Information Units to make them available for later use.

The proposal comes in addition to the obligation on air carriers to transfer advance passenger information (API data) to competent national authorities in charge of improving border control and combating illegal immigration according to Directive 2004/82/EC for EU-bound flights. This so-called API Directive also excludes intra-European flights.

---

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

3 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted in Strasbourg on 28 January 1981

4 Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007 and opinion 6/2004 on the implementation of the Commission decision of 14.05.04 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.

The EU DPAs welcome the initiative taken by the Commission to come to harmonised provisions given that third countries and individual Member States have already introduced their own systems analysing passenger data which might result in incompatible technical solutions and diverging data protection regimes. The proposal is complementary to the provisions of the Schengen Convention and the VIS II which are among others EU-wide means to curb illegal activities.

However, a prerequisite for any proposal limiting rights and freedoms is that it shows that the measures proposed are demonstrably necessary. Art. 8 of the ECHR demands that necessity can only be demonstrated if the proposed measures are justified by a pressing social need and when they are in conformity with the principles of proportionality and subsidiarity. This means that any limitation of rights must relate to the purpose of the measures, and cannot be achieved by other, less intrusive means. The EU DPAs reiterate their view that analysis of necessity and purpose of the measures in light of the goals should give convincing arguments for the proposal. The pressing social need for the collection and analysis of PNR data for the purpose of preventing and combating terrorist offences and organised crime is not sufficiently substantiated in the proposal objectives. The examples stated on page 10 of the impact assessment are not sufficient arguments to prove the necessity for collecting and analysing PNR data.

Evaluation of the necessity and proportionality of the proposal can so far only be based on the experiences with the US PNR framework and in the UK. Given that only one joint review took place for the US agreement, and that the US has never conclusively proven that the vast amount of passenger data it collects is indeed necessary in the fight against terrorism and serious crime, such a lack of available information in this context makes it problematic if not impossible to assess the necessity, effectiveness and proportionality of the proposal. The only substantiated available information to this end indicates that primarily API rather than PNR data are used. Also, the implementation date proposed in Art. 17 of the proposal (31 December 2010) does not indicate an urgent need for an EU PNR regime.

In any event, it must be clarified what the operational need for the use of PNR data is, what the added value is in the light of three existing measures - the SIS, the VIS and the use of API data. To date no evidence has been shown that data other than API data are necessary in the fight against terrorism and organised crime. The EU DPAs are, therefore, not in a position to conclude that the establishment of an EU PNR regime is necessary. This is all the more the case in light of Directive 2004/82/EC which foresees the obligation on air carriers to collect and transmit API data among others for combating illegal immigration, which is considered in most Member States a law enforcement activity. This Directive is not yet fully in force in some Member States and no impact assessment could be carried out substantiating the need for additional data other than biographical data contained in passports. The EU DPAs would have wished for a thorough analysis of how API data are being used by the competent authorities for the purposes stated in the Directive before further demands were made. The proposal itself says on page 3 of its explanatory memorandum that API data "**may** also help to identify known terrorists and criminals". If not even the value of API data can be proved how can the need for a vast amount of additional data be substantiated?

Under these circumstances, the EU DPAs remain unconvinced of the need for this intrusive development.

With a view to their advisory tasks, the EU DPAs shall, despite this position, examine and analyse the content of the proposal in order to facilitate an in-depth debate by the Council and other stakeholders.

1. Effectiveness

The proposal is limited to air carriers flying into and out of the EU. It leaves out any other mode of transport like road, rail and ship. It excludes flights within the EU unless they are part of an international flight. According to the proposal Member States have no discretion to extend the scope to national flights. It covers PNR data of passengers to the extent that they are contained in the computerised reservation and departure control systems of air carriers which means that carriers without electronic systems such as some charter airlines are excluded from the proposal. The EU DPAs question how the proposal can be proportionate and effective if it is not applied universally to all air carriers and other forms of transport.
Additional data elements are required for minors under 18 (see section 8).

2. Purpose limitation

The proposal regulates making available PNR data of passengers of international flights (i.e. excluding intra-EU flights) by air carriers to the competent authorities of EU Member States, for the purpose of preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them (Art. 1). The meaning of terrorist offences and organised crime is further defined in Art. 2, (h) and (i).

According to the explanatory memorandum and Art. 3 of the proposal, the data are considered a very important tool for carrying out risk assessment and for obtaining intelligence. As it is not clear how the data will be used for such risk assessments and whether they will be matched against other data available to law enforcement agencies and intelligence services, additional information is necessary. It has also to be observed that in many Member States for constitutional reasons intelligence services have no law enforcement functions and it is unclear how they will use PNR data.

3. Passenger Information Unit (PIU)

The proposal favours a decentralised solution for receiving personal data over a single European entry point. Such a decentralised solution might from a data protection point of view be a better approach, but might also entail diverging data protection levels and varying technical systems in different Member States. In the case of a decentralised system it has to be made sure that appropriate and consistent safeguards are in place which requires the involvement of the competent supervisory authorities. Further clarification is needed as to the responsibility of data protection authorities in cases where Member States co-operate to set up a joint PIU.

In Art. 3 of the proposal the decentralised solution envisages a Passenger Information Unit in each Member State that will be responsible for collecting and analysing PNR data it receives from carriers or intermediaries, and for carrying out the above mentioned risk assessment. The criteria and guarantees for this risk assessment are to be governed by national law. It is not clear what national law is referred to and whether it should be new or existing legislation. The EU DPAs warn that this reference to national law may lead to diverging national practices mentioned before. This approach might go against the objective of harmonisation of the Framework Decision. In any event, the EU DPAs stress that it is necessary that in this case the national data protection provisions are taken into account and that the supervisory authorities closely collaborate on all related questions.

4. Competent authorities

Art. 4 of the proposal establishes that Member States shall adopt a list of those competent authorities entitled to receive PNR data from the Passenger Information Unit. According to the EU DPAs, these authorities should only include **law enforcement** authorities responsible for the prevention or combating of terrorist offences and organised crime. The EU DPAs stress that the competent authorities may have several national functions, for example, law enforcement activities and collecting intelligence. The proposal should therefore make sure that within these authorities restrictions are put in place with regard to the purposes set out in the proposal.

5. Method of transfer

The EU DPAs welcome the fact that Art. 5 of the proposal sets out that carriers should use the push method as a method of transfer of PNR data. The EU DPAs would like to stress that the technical measures to ensure the push method should be commonly agreed. Air carriers should in any case be involved in this context and advice from data protection authorities as well as IT specialists should be ensured. It is not clear how individual PIUs will deal with all those carriers that are established outside the EU and which do not yet have the technical means to push data so data have to be pulled from many different systems. It is not clear either how to get data from carriers that do not run electronic reservation systems. In case data have to be pulled and the air carrier of a third country does not agree on such an access by the PIU of a Member State, questions of enforcement have to be dealt with as well.

Air carriers should be obliged to move to one specified push system as soon as possible to guarantee a uniform approach. The push method is from a privacy point of view the only acceptable one and for that reason the pull method should not exist along the push system. The EU DPAs also consider it important that the negative experience the EU has had to date with regards to the change from pull to push in the case of the US PNR agreement, which still has to occur, should be taken into account when developing the push system. All technical questions should be solved together with all parties involved before the final implementation of the push system. Any pull system before a push system should be categorically excluded.

Alternative less privacy invasive systems, such as risk assessment based on pseudonymised data, have not been assessed although the amount of personal data transferred to competent authorities could be dramatically reduced by these systems. The EU DPAs are aware that such systems exist and would like to see them considered.

6. Exchange of information

The EU DPAs are also concerned by the reference to international agreements in Art. 8.2 and the consequences of automatic reciprocity with third countries using a PNR system. It has to be acknowledged that the fact of an existing European PNR regime might lead to PNR demands on the basis of reciprocity by undemocratic or corrupt regimes as well. It will be difficult to counter such demands. Therefore it has to be asked whether the consequences of reciprocity have been considered sufficiently. (E.g. credit card information which is quite often part of a PNR in the hands of civil servants of a state which is not able to abolish corruption might become a serious problem. Further, the understanding of the wording “fight against terrorism” in some states might differ significantly from the European view. Reciprocity could enable a dictatorship to carry out a risk analysis on dissidents on the basis of PNR. Finally, it cannot be foreseen how undemocratic states will handle the results of a PNR risk analysis and whether passengers will have any rights (not only data protection rights) in this context.

Furthermore, the proposal leaves open the question whether PNR data to be transferred to third countries may be exchanged on a bulk basis or only on a case-by-case basis. It is not clear which data protection regime applies in third countries, for example retention periods, dissemination of information, reviews and technical security aspects. Furthermore, the questions of how the data subjects will be informed of the transfer of their data to a third country and how they can exert their legitimate rights remain. Finally access by a third country to passenger data held in European reservation systems in a pull method as a means of reciprocity is not acceptable. It would be impossible, for instance, to imagine that a country without any protection of privacy could by way of reciprocity have access to the European reservation system Amadeus by pulling all data available on in- and outbound flights. These issues should be addressed and solved prior to the adoption of the Framework Decision. From a privacy point of view transfers should only be possible on a case-by-case basis.

7. Retention period

The EU DPAs reiterate that any substantiated retention period should be founded on clearly justified needs of processing of the data, be proportionate and in line with acknowledged data protection standards which stipulate that data should no longer be stored than is necessary for the purposes for which they were collected or for which they are further processed. According to Art. 9 of the proposal, data provided to the Passenger Information Unit shall be retained for a period of five years and then for a further period of eight years, i.e. 13 years taken together. The EU DPAs are of the view that the need for the proposed retention period has not been substantiated, nor does the proposal provide any reasoning with regard to proportionality of the proposed retention period. The 13-year retention period is thus disproportionate for the stated purposes and not acceptable.

The retention period is not even consistent with other European instruments introducing retention periods for similar purposes. For example, Directive 2004/82/EC on the transfer of API data states that the data should be deleted 24 hours after arrival; Directive 2006/24/EC on the obligation of electronic communications service providers to retain traffic data foresees a retention period of up to two years.

On the other hand any comparison to the EU-US PNR agreement in this context cannot apply because of the apparent lack of proven necessity or justification for the required retention period of 15 years in that agreement.

In this context the Article 29 Working Party reiterates that it already deemed the 3.5-year retention period of the first PNR agreement with the US of 2004 quite long.

The PNR agreement with Canada has the same retention period of 3.5 years. A joint review - that is still to be organised - might yield findings as to the proportionality of this retention period.

8. Data elements

The list of data elements contained in the annex of the proposal is closely modelled on the EU-US PNR agreement signed in July 2007. It contains all 19 sets of data elements mentioned in the agreement albeit in a slightly different order. As already expressed in the Article 29 Working Party opinion 138 on the EU-US PNR agreement, these sets put together certain data elements which appear to conceal the fact that in reality it is not 19 data elements that are transferred, but at least around 35 individual elements as far as they are contained in the air carriers' electronic reservation and departure control system(s).

The EU DPAs consider this list of data sets excessive as there is no explanation given why so many data elements are required in the fight against terrorism and organised crime. The proposal seems to take it for granted that these sets are considered useful as the US authorities do, but gives no further evidence as to their necessity. The EU DPAs recall that data mining is not a stated objective of the proposal.

It also has to be mentioned that the data element "language(s) spoken" could be a sensitive data element revealing the ethnic origin of the minor and would have to be deleted anyway.

While some PNR data are put into the departure control system by the air carriers prior to the departure, such as baggage information and seat number, other details are provided by the passenger when booking the flight, such as travel itinerary of frequent flyer information. Unlike API data, PNR data other than data contained in the departure control system cannot be considered validated information. Such PNR data are given by each passenger on a voluntary basis in the process of booking a certain flight. They might be provided by the passenger even on an arbitrary basis, for example, when ordering a specific meal. The air carriers are not in a position to verify the details provided nor are they obliged to do so. Therefore, they cannot be held accountable for the accuracy of such PNR data. Apart from the fact that PNR data for each passenger are in most cases very limited, they are unchecked and it has to be questioned how they can be considered a reliable source of information in assessing risks. The EU DPAs are, therefore, not convinced that the list of required data elements is necessary for the stated purposes. They consider the list excessive and calls on the Council to curtail this list. They note in this context that the PNR agreement with Canada foresees only 25 individual data elements considered sufficient in the fight against terrorism and organised crime.

The EU DPAs are also concerned at the fact that the list of data sets might contain information on third parties, such as the employer, partner or relatives of the data subject, for example, when giving contact details, billing address or details on the departure and arrival agent. The third party is in most cases not aware of the transfer of personal data to the Passenger Information Unit and can, therefore, not exercise his or her rights.

9. Sensitive information and filtering

Art. 3 and Art. 6 of the proposal explicitly foresee the immediate deletion of sensitive data which could reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sex life of individuals either by the Passenger Information Unit or the proposed intermediary. The list of data elements in Annex 1 of the proposal does not include sensitive data but such data might be contained in data fields 12 "General remarks" and 19 "all historical changes to the PNR listed in numbers 1 to 18". As mentioned before also the language(s) spoken by a child could reveal his ethnic origin.

The EU DPAs note that one of the main principles of data protection is the controller's responsibility for the processing of personal data, such as is enshrined in Directive 95/46/EC (Art. 2 d) in combination with Art. 6 (2). Similar provisions can be found in Art. 2 (d) and Art. 5 of Convention 108. It should, therefore, be up to the air carriers to filter sensitive data out before transmitting them in a push system to an intermediary or the Passenger Information Unit. Before considering the filtering of sensitive data, clear reasons should be given why fields containing such sensitive information in the list of data elements are necessary at all. The EU DPAs reiterate that the PNR agreement with Canada does not include any data elements which might contain sensitive information.

Having said this, the EU DPAs consider it contrary to accepted data protection principles that the proposal absolves the data controller i.e. the airlines of their responsibility to filter out sensitive data which are not part of the list of required data elements.

The proposal leaves unaddressed the question of how the intermediaries and the Passenger Information Units will come to a common understanding of sensitive data and how they have to co-operate on this question which is not a purely technical one. It is also important to note that the notion and relevance of sensitive data might change over time and that for that reason it is necessary to continuously identify new relevant sensitive data.

The EU DPAs call on the Council to curtail the list of data elements in such a way that the filtering of sensitive data elements will no longer be necessary. If the Council, however, will not revise the list, the filtering of sensitive data should be left to the air carriers which should engage with their supervisory authorities and the Commission to identify all relevant sensitive data and keep an updated list. Such an approach will not only take account of accepted data protection principles but will also guarantee an efficient and uniform approach to this question.

10. Data protection provisions

The data protection provisions as contained in Art 11 of the proposal refer to the draft Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters which has still to be adopted.

It is not clear in what way the draft Framework Decision on Police and Judicial Co-operation could provide the appropriate protection as its scope will be reduced to the transfer of data between the law enforcement agencies of Member States. The proposal, however, has a different scope as it governs the transfer of passenger data by air carriers to the PIUs. The lack of clear data protection provisions is unacceptable and in any event needs to be remedied.

The EU DPAs consider the mention of specific and clear provisions indispensable as not all Member States have included police and justice in their transposition in national law of Directive 95/46/EC. The EU DPAs propose therefore to include those provisions in the proposal instead of referring to another legal instrument. These provisions should among others regulate the rights of data subjects such as the right to access, correction of data and redress. This would enhance transparency and facilitate the protection of data subjects.

11. Information to data subjects

In Art. 5 (6) of the proposal Member States are given the task to make sure that carriers inform passengers about: the provision of PNR data to the Passenger Information Unit (and, where applicable, the intermediary); the purposes of processing; the period of data retention; their possible use to prevent or combat terrorist offences and organised crime; and the possibility of exchanging and sharing such data.

The EU DPAs note with great concern that no mention is made of to whom the data subject has to address, or how the data subject can exercise his or her rights, notably the right of access. The EU DPAs stress that such a provision is fundamental and recommend incorporating this much needed text into the proposal.

Furthermore, it is necessary to regulate how the supervisory authorities of the Member States will enforce the right to information, what sanctions there will be, and imposed by whom, if carriers, intermediaries and Passenger Information Units do not properly inform passengers. The Article 29 Working Party would like to recall that it has in the past issued two opinions[5] to give guidance to air carriers and to raise awareness among the travelling public. The EU DPAs also consider it necessary in the case of the EU PNR regime to come to a harmonised approach which takes account of all stakeholder concerns.

12. Data security and encryption standards

Art. 12 of the proposal relates to security measures to be taken by the Passenger Information Units, intermediaries and competent authorities. In order to be complete, this provision should also contain reference to necessary organisational measures to be taken, such as the training of staff and disciplinary measures when security measures are not complied with.

From Arts. 13, 14 and 15 it appears that the Committee mentioned in Art. 14 will advise in the setting up the common protocol and the encryption standards. Advice from experienced data protection authorities as well as IT specialists in these matters should be foreseen in the Framework Decision.

The EU DPAs would like to stress that using secure methods is essential and should not be postponed. Art. 15 should therefore in any event include that moves towards the common approach must be encouraged and that any delay in securing the mode of transmission needs to be substantiated.

13. Statistical data

The EU DPAs welcome the fact that the proposal contains provisions on statistical information. Information on the number of subsequent law enforcement actions involving the use of PNR data may prove to be valuable (and could possibly provide arguments for the necessity of the use of PNR data or modifications of the regime). It is also welcome that these statistics will not contain any personal information which requires an accurate and immediate anonymisation. Common rules for anonymising should be worked out before the system is operational.

14. Review and sunset clause

The EU DPAs welcome the fact that the Commission will undertake a review of the proposed Framework Decision. The EU DPAs are, however, concerned at the fact that no mention is made of independent supervisory authorities or external experts. The EU DPAs stress the need for them or their representatives to be fully involved in any conclusive review, both in the preparation and in carrying out the review.

Provisions on when and how the review process will be prepared and carried out should be clearly provided for in the proposal. The EU DPAs also strongly recommend that the review report also be submitted to the European Parliament.

---

5 WP 97 "Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America" adopted on 30 September 2004 and WP 132 "Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities" adopted on 15 February 2007 and a "Short notice for travel between the European Union and the United States"

The EU DPAs expect the review to be conducted on a regular annual basis and that recommendations are made as to the improvement of the system and to all privacy related matters.

Given that the Framework Decision will have far-reaching consequences for all travellers into and out of the EU, the EU DPAs consider it necessary to thoroughly analyse and evaluate the necessity of such a measure after a certain period of time with the participation of independent experts. Such a comprehensive in-depth assessment cannot be done during a review as foreseen in Art. 17. The EU DPAs, therefore, propose to introduce a sunset clause which mandates a thorough evaluation of the provisions of the Framework Decision, their effectiveness and their justification before any extension of the scheme. Such an evaluation should be carried out together with independent experts.

15. Other harmonisation aspects

In this opinion the EU DPAs have several times called for a harmonised approach to avoid a diverging transposition of the Framework Decision in the Member States. Some issues in this field remain.

The proposal permits Member States to continue to apply, or to conclude, other bilateral or multilateral agreements, in so far as such agreements enhance or facilitate the objectives of the proposal. According to the EU DPAs, these provisions run contrary to the aims of the proposal, namely ensuring harmonisation in this area.

It also has to be mentioned that the explanatory memorandum clearly states that the Framework Decision leaves as much scope as possible to national decision makers to implement the provisions. It is for the Member States to decide on **how** and where to set up their PNR system and its technical aspects. The harmonisation aspects are only limited to those strictly necessary. This might not be enough. It has to be feared that diverging interpretations in various Member States will occur and that air carriers and data subjects are confronted with different systems and standards. In this context the EU DPAs regret that Directive 2004/82/EC has not yet been fully implemented by some Member States although the deadline for implementing the Directive has long expired. No impact assessment could be carried out to analyse the technical and data protection aspects of national regulations transposing Directive 2004/82/EC. Up to now not even experiences are available of how Member States have used their right to discretion and whether further harmonisation is necessary as to the transposition of that Directive. Such experiences would now be highly welcome in assessing the degree of discretion necessary and desirable to Member States as to the transposition of the current proposal.

The EU DPAs are of the view that a situation where air carriers and data subjects are faced with diverging systems and approaches is not acceptable. They, therefore, are in favour of setting up a forum which will allow for an exchange of ideas and best practices between Member States to avoid diverging risk assessments. Such a forum, to include data protection authorities, should also be used to elaborate on all other issues related to the implementation of the Framework Decision.

III Conclusion

The proposal brought forward by the Commission will deeply affect all travellers flying into or out of the EU. It comes in addition to the obligation of collecting fingerprints when applying for a passport or a visa. It will have consequences for the airline industry, reservation systems and law enforcement agencies alike. If the current version of the draft Framework Decision is implemented, Europe would take a great leap forwards towards a complete surveillance society making all travellers suspects. As already in the case of traffic data retention (Directive 2006/24/EC), a vast

amount of personal data will be collected by private entities and stored for possible later use by government agencies despite the fact that the effectiveness and necessity of such a system has never been proven. The collection of data affects all travellers whether they are under suspicion or, as in most cases, innocent citizens, and allows the reconstruction of their travel patterns for many years. For these reasons serious doubts remain whether the approach chosen by the EU to put all travellers under general surveillance and to consider them suspects in the fight against terrorism and organised crime is the right way to tackle these phenomena. In particular it has to be stressed that there is no experience yet as to the use of API data in the fight against illegal activities.

Overall, the EU DPAs are of the view that this proposal takes a more measured approach than previous arrangements on this topic, in particular the recently signed EU-US PNR agreement, and that the purposes have been specified and limited to preventing and combating terrorism and organised crime. It takes into account some of the Article 29 Working Party's concerns as stated in the joint answers to the questionnaire given in January 2007. However, other concerns remain and have to be addressed. In particular the necessity of the proposal, as required by Art. 8 ECHR which remains insufficiently demonstrated. Unlike API data, PNR data are not validated data and must be considered unreliable. In addition, the proposal fails to give any details of the rights of passengers and does not specify any safeguards. It refers only to the Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation which has not yet been adopted and the data protection provisions of which are still unclear. Although a European approach is preferable to national initiatives in this field, it has to be noted that the proposal gives wide discretion to Member States and it has to be feared that the interpretation of the Framework Decision will vary and its implementation will not be carried out in a uniform way. The proposal neither clearly specifies what risk assessment means nor how the data collected will be used for intelligence purposes. This needs further consideration.

The data elements listed in the annex of the proposal must be considered excessive and the retention period of 13 years disproportionate.

The EU DPAs welcome the preference for a "push" method of transmitting the data. They are of the view that the "push" should be the only acceptable way of transferring passenger data which should not be left to the discretion of non-EU carriers. From a data protection point of view all carriers should be treated in the same way whether they are based in Europe or elsewhere.

As to sensitive data the EU DPAs welcome that they have to be filtered out but maintain that this task should be given to data controllers rather than to third parties. The involvement of the supervisory authorities as to the definition of sensitive data is crucial in particular given the experience gathered through their participation in the activities of third pillar Joint Supervisory Authorities.

Given these shortcomings the EU DPAs consider it indispensable that there is a serious debate on such a wide-ranging measure with deep privacy implications including the European Parliament, national parliaments and all stakeholders involved in the development of such a system, in particular the airline industry and the reservation systems. The EU DPAs consider it all the more important to find a well balanced privacy-enhancing solution because, due to the political and economical weight of the EU, any future EU PNR regime will certainly set a precedent to other countries around the world which are still contemplating the introduction of a similar scheme and might follow suit. The EU should not miss the opportunity to set high privacy standards in this field.

The EU DPAs will continue to provide input and expertise. In this respect, both the Article 29 Working Party and the Working Party on Police and Justice remain available to the Commission and the Council in their capacity as independent advisory bodies of data protection experts. The Article 29 Working Party also looks forward to being involved in the implementation of the Framework Decision in relation to the impact on carriers, who have obligations under Directive 95/46/EC.

Done at Brussels,
on 5 and 18 December 2007

For the Art 29 Working Party	*For the Working Party on Police and Justice*
The Chairman	The Chairman
Peter SCHAAR	Francesco PIZZETTI