COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2007
SEC(2007) 1453

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

COUNCIL FRAMEWORK DECISION

on the use of Passenger Name Record (PNR) for law enforcement purposes

IMPACT ASSESSMENT

{COM(2007) 654 final}
{SEC(2007) 1422}

TABLE OF CONTENTS

Impact Assessment

On A Common Approach to the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

On 5 September 2007, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. In the opinion, the Board in brief stated that the IA report should be further improved by better illustrating the risk of no EU action, by explaining in more detail the choices made in shaping and selecting the preferred policy option, and by elaborating on the consequences for relations with third countries.

It further stated that:

(1) The limitation of the scope to extra-EU flights should be better explained.

(2) The choice of the preferred option should be better explained.

(3) Impacts on relations with third countries should be further elaborated.

(4) The problem definition should be strengthened by illustrating the risk of divergent national measures.

The present version of the Impact Assessment report has been significantly redrafted, with a view to taking these recommendations fully into account. Additional information and modifications have been introduced to this end in many of its sections.

1.1. Organisation and timing

Work on the Common Approach to the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes commenced in 2005 following several calls to that effect by the European Council. More specifically, the European Council in its Declaration on combating terrorism of March 2004 called on the European Commission to bring forward a proposal "*for a common EU approach to the use of passengers' data for border and aviation security and other law enforcement purposes".* A European policy in this area has been announced in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003[1]. The request for European action on PNR was repeated in the Hague Programme and by the extraordinary JHA Council of 13 July 2005 in its Declaration on the EU response to the London bombings of July 2005. More recently, the EU Action Plan on combating terrorism calls for the development and implementation of the exchange and analysis of airline passenger name records (PNR).

In this context, the Commission has also actively participated in the work of the International Civil Aviation Organisation (ICAO) to establish guidelines for the use of PNR data.

1.2. Consultation and expertise

Several meetings and consultations were organised under the negotiations on the transfer of PNR data to the United States and on the transfer of Advance Passenger Information and PNR data to Canada. Further to the meetings organised by the Commission services with associations of air carriers and representatives of computer reservation systems, three

[1] COM(2003) 826.

dedicated meetings on a possible initiative on the development of an EU policy on the use of passenger data have been organised by under the umbrella of the Forum on the prevention of organised crime. These meetings brought together representatives of data protection authorities, border control and law enforcement authorities, and Europol, and took place in November 2003, May 2005 and July 2005.

For the purposes of the preparation of this report, the Commission services further consulted all the relevant stakeholders on the basis of a questionnaire which was sent out in December 2006. Subsequently, the Commission invited one representative of each Member State, who could be accompanied by an expert, to a meeting in Brussels on the 2nd February 2007, during which the representatives of the Member States had the opportunity to exchange their views.

The questionnaire was sent to:

- All the Member States
- The data protection authorities of the Member States
- The European Data Protection Supervisor (EDPS)
- The Association of European Airlines (AEA)
- The Air Transport Association of America
- The International Air Carrier Association (IACA)
- The European Regions Airline Association (ERA)
- The International Air Transport Association (IATA)

Replies were received from 24 Member States, namely Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. Such replies were sent either by the Ministry of the Interior or the Ministry of Justice of the Member States, whichever was responsible for the file. A joint reply was received from the national data protection authorities of the Member States. Replies were also received from the EDPS, the Air Transport Association of America, the International Air Carrier Association (IACA), the Association of European Airlines (AEA), the European Regions Airline Association (ERA), the International Air Transport Association (IATA), LOT Polish Airlines and Austrian Airlines. A table summarising the replies of the Member States is attached as **Annex B** hereto.

Furthermore, extensive discussions were held with air carriers, data protection authorities and border and law enforcement authorities since 2003, notably between 2003-2004 and in 2006 during the negotiations for the agreements on the transfer of PNR data to the US and during the years 2004-2005 for the agreement on the transfer of PNR and API data to Canada. The implementation of the PNR agreement with the US has been the subject of a joint review between the Commission, assisted by national authorities, and US authorities.

The data protection authorities of the Member States, meeting as a consultative body to the Commission under the umbrella of the Article 29 Working Party, have issued a number of opinions on the use of PNR data[2].

---

[2] Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, January 2005, Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data

A steering group has been set-up to steer the group of the impact assessment. The group consisted of officials from the various services of the Commission, it met once to discuss the issue and further comments where provided in writing.

1.3. Impact of the consultations

The replies that the Commission received to the questionnaire have had a major impact on shaping the present report and will have an impact on any legislative proposal that the Commission might submit.

More specifically, such impact affected:

- *The choice of the policy option*: it became clear from the replies which were received to the questionnaire that most of the Member States are clearly in favour of a legislative instrument which would regulate a common EU approach on the matter. The Art.29 Working Party was not convinced of the necessity of such a proposal and is therefore opposed to the proposal, but it noted that once the necessity is established or several Member States would be considering the development of a national PNR systems, then harmonisation of such measures at an EU level should be preferred.
- *The scope of the proposal as regards the modes of transport*: the majority of the consulted parties agree that the scope of the proposal should be limited to air transport as a first step, with the possibility of extending it to other forms of transport at a later stage. This approach is generally based on the fact that air carriers/operators already have systems with which they capture PNR data and it would therefore be easier for them to comply with the proposal.
- *The geographical scope of the proposal*: most parties consulted believe that the geographical scope of the proposal should be limited to flights from third countries to the EU and from the EU to third countries. At this stage, it is thought disproportionate to extend the scope of the proposal to flights from one Member State to another Member State and to internal flights within a Member State.
- *The use of and purpose for collecting the PNR data*: The collection of PNR data should be used for the purposes of the third pillar only, i.e. the prevention of and fight against terrorism and related crimes and organised crime.
- *The data retention period*: It was commonly agreed that, for the system to be effective, the data need to be retained for a period of 5 years, unless they were used for a crime investigation or an intelligence operation.
- *The body receiving the PNR data*: The majority of the Member States are in favour of the idea that the data be received by a Passenger Information Unit which will be identified within each Member State, while other Member States are in favour of a centralised EU Unit which would receive data from carriers from all the Member States.
- *The method of data transmission*: The "push" method of transmission is preferred to the "pull" method by all parties consulted. The main difference of the two methods is that in the "push" method, the data are being transmitted by the carrier to the national authority,

---

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, June 2004, and others.

whereas in the "pull" method the national authority obtains access to the reservation system of the carrier and takes the data.

- *The onward transfers of the PNR data*: Most of the consulted parties are in favour of the PNR data being transmitted to the national competent authorities and to the competent authorities of other Member States. Some Member States are in favour of the data being transmitted also to the competent authorities of third countries.
- *IT security*: For the purposes of security in the transmission of the data, most parties which were consulted agree that common encryption standards could be adopted to ensure such security.

The choice of dealing with the issue by means of encouraging cooperation between the Member States was one which was considered initially but rejected by all, except two parties consulted. Such encouraged cooperation could be in the form of exchange of best practices. However, it is considered that the option of encouraging co-operation between the Member States, would not achieve the desired objectives, for the following reasons:

- It would be extremely difficult, if not impossible, to ensure a common EU approach on the matter in this way, and it would be impossible to ensure that such best practices are actually exchanged.
- Further, the problems of terrorism and organised crime affect most of the Member States and are not limited to some Member States only. Because of the open internal borders within the EU, in case that some Member States refused or failed to co-ordinate their activities, they would create a substantial loop-hole to the security of the Union which we are aiming to increase. The security of the EU is the joint responsibility of the Member States and all Member States should act in a harmonised manner in order to achieve results. The goal of increasing security cannot be sufficiently achieved merely by encouraging co-operation between Member States. Such encouraged cooperation would not contribute towards achieving the objectives of Article 29 of the Treaty on European Union, i.e. "… to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States in the fields of police and judicial cooperation…".
- The airlines and the data protection authorities of the Member States, even though against the general idea of making available PNR data for law enforcement purposes, were adamant that if any action is taken, then that should lead to harmonisation. Otherwise, we expect to end up with diverging requirements which will be ultimately very costly for the airlines and the Member States. It would be very costly for air carriers if, for example, they have to send 20 PNR elements to the UK, 25 to France and all to Denmark, retain the data on behalf of one Member State but not for the others, use different encryption standards and protocols for each Member State in order to safeguard the secure transmission of the data.
- It is further noted that the guidelines of the International Civil Aviation Organisation (ICAO) on PNR data are not binding and have proved not to provide a sufficient basis for the required co-operation.
- On the basis of the above, the option of encouraging co-operation between the Member States in this field is rejected at this initial stage and will not be further examined.

2. PROBLEM DEFINITION

2.1. Description of the problem

Terrorism currently constitutes one of the greatest threats to security, peace, stability, democracy and fundamental rights, values on which the European Union is founded, as well as a direct threat to European citizens. The threat of terrorism is not restricted to specific geographic zones. Terrorists and terrorist organisations can be found both within and outside the borders of the EU and have proved their ability to carry out attacks and acts of violence in any continent and against any country. The "EU Terrorism Situation and Trend Report 2007" of Europol identified that almost all terrorist campaigns are . It is clear that the internal and external aspects of the fight against terrorism are interlinked and that, for any measure to be effective, a close cooperation and an enhanced exchange of information between Member States and their respective services, as well as with Europol and, where appropriate, the competent authorities of third countries, is necessary.

The Europol "EU Terrorism Situation and Trend Report 2007" notes that there were 498 reported terrorist attacks in the EU in 2006. The Report identifies that, although there were no successful Islamist terrorist attacks in the EU in 2006, the type of the attempted attacks shows that the attacks are aimed at indiscriminate mass casualties and at the transportation infrastructure of the Member States.

The same Report notes that 706 individuals were arrested in the EU in 2006 on suspicion of terrorist offences, out of which 257 were arrested in relation to Islamist terrorist attacks. The Report concludes that investigations into Islamist terrorism are clearly a priority for Member States' law enforcement. The acquittal rate at the trial stage for terrorism charges was recorded at 15% in 2005 (similar data for 2006 are not yet available).

As regards organised crime, over the last few years the European Union and the world have experienced more than ever before its geographic spread. Criminals have taken full advantage of the effects of globalisation and are using more and more opportunities to travel, exchange information and communication to perform their business. Intelligence has further indicated that, due to the increasing access that law enforcement authorities have to e-communications, terrorists and criminals tend to prefer to travel and meet to discuss their business rather than communicating long-distance. It is becoming therefore, more and more important to obtain as much information as possible about the travel of such persons.

After 9/11 the US proceeded immediately with the introduction of PNR legislation. Even though the EU had agreed initially in 2004 to make PNR data available to the US, it has been more reluctant to introduce such measures itself internally. Since then, and because the terrorist threat remains and is even intensified, the Member States of the EU are realising more and more the need to raise their level of awareness of this threat. At this point, it seems appropriate to proceed with the introduction of PNR legislation and the Member States indicate that there is a strong need for the EU to take proactive, rather than solely reactive, measures in order to combat terrorism and organised crime effectively.

This impact assessment aims to assess whether there is a need for a proposal at European Union level aimed at setting up a coherent legal framework regarding the obligation of carriers to transmit Passenger Name Record (PNR) data to the relevant competent authorities for the purposes of preventing and fighting terrorist offences and organised crime. Such a measure would aim to contribute towards building intelligence about terrorists and criminals and to identifying behaviour patterns of such persons. The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism notes, for example, the importance of

identifying persons who travel to conflict zones in order to prevent terrorist training. To that extent, the proposed measure would aim to identify both terrorists coming from outside the EU as well as those already in the EU. Such a measure could also contribute towards depriving terrorists and criminals of the opportunity to travel and enter the territory of the EU and towards preventing the means of transport themselves to be used as weapons. The measure could further contribute to making transport safer, and enhancing legitimate travel.

Currently air carriers have an obligation to communicate Advance Passenger Information (API) to the competent authorities of the Member States, under Council Directive 2004/82/EC[3]. This measure aims to provide a means to border control authorities to enhance border control and to fight illegal immigration. Under this Directive, Member States are obliged to take the necessary national measures to ensure that carriers transmit, at the request of the authorities responsible for carrying out checks on persons at external borders, information concerning the passengers of a flight. Such information includes only the API Data, which is basically biographical data. Such data include the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport and the initial point of embarkation. The information contained in the API data may also help to identify known terrorists and criminals by running their names against alert systems, such as the SIS.

PNR data include passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences and other information. The PNR data of a certain passenger usually does not contain all PNR fields, but only those that are actually provided by the passenger at the time of the reservation and information received upon check-in and boarding. It must be noted that air carriers already capture the PNR data of passengers for their own commercial purposes, but that non-air carriers do not capture such data.

Currently, the competent authorities of the Member States may obtain the information which is contained in the PNR data of a passenger of an international flight by looking at his ticket and the boarding card that he is required to fill in for the purpose of border control. It is only in very rare cases that the PNR data of a passenger, as processed in the reservation system of the carrier, will contain some additional information. The added value of the proposal would be that the competent authorities of the Member States would be able to receive the data in an electronic form and well in advance of a flight's arrival. This will provide the authorities with the possibility of processing it electronically and in substantially less time than if it were done manually. This, in turn, is beneficial both for the authorities as well as the passengers since it reduces the time that they have to wait for border control.

PNR data can be used by law enforcement authorities in five ways:

- Running the PNR data of passengers against alert systems in order to identify known terrorists and criminals
- Once a known terrorist or criminal is identified, PNR can be used to identify another passenger who is connected to the known terrorist/criminal. This can be done by comparing the PNR data of the known terrorist/criminal to those of other passengers and identifying those who might share the same address, credit card number, contact details etc with him. This exercise can be very useful in obtaining evidence by association and in identifying previously unsuspected passengers.

---

[3] OJ L 261, 6.8.2004, p. 24.

- Running the PNR 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.
- Running the PNR data of passengers against risk intelligence relevant at a certain time, with the aim of identifying high-risk passengers. For example, when intelligence exists that a travel agency in a certain country has connections with a specific terrorist organisation or criminal group, PNR data can help identify which passengers have bought tickets from such suspected agency.
- Providing intelligence on travel patterns and associations after a terrorist offence has been committed.

For the purposes of the fight against terrorism and organised crime, the information contained in the API data would be sufficient for the first purpose mentioned above, i.e. for identifying persons by using alert systems. API data are official data, as they stem from passports, and sufficiently accurate as to the identity of a passenger. The advantage however, that PNR data has over API data for this purpose, is that PNR data can be available much earlier than API data. In case therefore, that PNR reveals that a highly dangerous person will be on a certain flight, measures can be taken to prevent that person from boarding the flight. On the contrary, if only API data are available, that person is already on the flight in which case there are two alternatives, none of which is sufficiently satisfactory: first, to make the airplane redirect or turn back, or secondly, deal with the dangerous person upon arrival. On this basis, it is clear that the provision of PNR data would provide an advantage to the mere provision of API data.

As regards the other four uses of PNR which are mentioned above, it is clear that API cannot be put to any of those uses. API data cannot provide characteristics and patterns of behaviour of passengers, cannot provide evidence by association and cannot be run against intelligence. As such, API data are unable to help identify unknown high-risk passengers.

The rationale behind identifying unknown high-risk passengers is that this allows for secondary screening upon their arrival and to further questioning by border control officers and in specific circumstances, in combination with other information, to a refusal of entry in the territory of the destination country. On the other hand, low-risk and unsuspected passengers are subjected to minimum border controls.

For the purposes of the fight against terrorist offences and organised crime, the use of PNR data in combination with API data is an especially useful and necessary one, especially in obtaining evidence by association. Without the API data, PNR data would be unable, in themselves to provide the behavioural analysis and to be used for obtaining intelligence and evidence by association. A case of obtaining evidence by association would be for example when a known terrorist who is identified by his API data, travels together with another person who has used the same credit card for purchasing the ticket, or used the same home address etc. Further, the examination of the travel patterns of certain suspected passengers during a period of time can help point towards possible planned attacks. Information linked to travel prior to and in preparation of an attack can also provide essential data for law enforcement purposes.

As stated above, API data are currently transmitted (or should be transmitted once the Council Directive 2004/82/EC is transposed in all Member States) only by air carriers and only for international flights. Therefore it is advisable that any proposal for the use of PNR data should also be limited to air carriers operating international flights. However, it might be useful in the future to consider the extension of the scope of the API Directive to further cover at least sea travel, at which point the PNR data collection could also be extended.

Currently, arrangements for the transmission of PNR data in the context of the fight against terrorism and organised crime have been concluded between the EU and the United States and Canada and are limited to travel by air. This implies that air carriers, which were already capturing the PNR data of their passengers for their own commercial purposes, are obliged to transmit these data to the competent authorities of the USA and Canada. On the basis of an exchange of information with these third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has further been able to learn from the experiences of such third countries in the use of PNR data, as well as from the experience of the UK from its pilot project. The UK experience shows that, in the two years of working its pilot project (which covers only air and only limited routes), 12,044 alerts have been issued by the system, 1050 arrests for various crimes have been made and substantial intelligence has been obtained for a range of suspects The US has also indicated a successful operation of its system, with several arrests, identification of human trafficking networks and gaining of valuable intelligence.

Some Member States, namely the United Kingdom, France and Denmark, have already enacted primary legislation for the capture and use of PNR data, and are in the process of considering secondary legislation to implement such national PNR systems[4].

An analysis of the national legislation of the UK, France and Denmark indicates that their provisions are diverging and can be summarised as follows:

- The UK suggests the use of PNR data in the fight against terrorism and all crimes and illegal immigration. PNR will be required from all flights, including intra-EU and domestic flights. The period of retention of the data is not mentioned. There will be wide sharing of the data between its agencies. PNR will be required from air, sea and rail carriers to the extent that such exist.
- France suggests the use of PNR data in the fight against terrorism and illegal immigration (not for other crimes). PNR will be required from all flights, including intra-EU. The period of retention is 24 hours for immigration purposes and 5 years for terrorism purposes. PNR data will be required from air, sea and rail carriers to the extent that such exist.
- Denmark suggests the use of PNR data only in the fight against terrorism and crimes against the State. The proposed period of retention is 1 year and covers only air travel. It does not proposes a system of transmission of PNR data but a system of retention of the data by the air carriers while giving direct access to such data to some law enforcement agencies. Informal talks with Denmark indicated that they are considering amending their legislation because the system of retention of the data by the air carriers is thought to be ineffective.

These provisions indicate that there is divergence as regards the purpose of the system, the period of retention, the structure of the system, the geographical scope and the modes of transport which are covered. It is also very likely that there will be divergence on the measures taken to safeguard the security of the transmission of the data, i.e. will introduce different encryption standards and transmission protocols.

It is interesting also to note that such legislation was enacted in the three Member States in the context of transposing the API Directive.

---

[4] For the UK, the Immigration, Asylum and Nationality Act 2006;
For Denmark, the Air Navigation Act;
For France, Article 7 Division IV et V - art. 8 de la loi n° 78-17 du 6 janvier 1978.

Furthermore, it can be anticipated that more third countries are likely to request the provision of PNR data from the EU directly or from individual Member States. For example Australia and New Zealand have already officially requested the conclusion of bilateral agreements with the EU for the provision of such data, and more third countries are expected to put forward such requests. The consultation has further indicated that more Member States will prepare their own legislative instruments regulating PNR data collection and transmission to their relevant authorities and/or third countries in the near future. Such a development might lead to the establishment of many and even potentially 27 considerably diverging systems. Carriers would be faced with the very difficult task of having to comply with a number of different systems, and the national authorities would have to develop systems to be able to receive and transmit data in potentially many different ways. For example, carriers would run the risk of having to transmit different PNR elements to different Member States, "push" them to some authorities and "pull" them from others. For this reason, the carriers associations which were consulted for the purposes of this report, were strongly in favour of harmonisation of the field at an EU level, rather than being faced with various diverging systems.

The issue of ensuring adequate protection of the privacy of the affected passengers is also one to be considered. As more and more Member States adopt national legislation for the transmission by carriers and use of PNR data and as more and more third countries request such transmission from carriers, it is important to ensure that the data are transmitted and used under adequate safeguards and with sufficient redress mechanisms for the passengers, rather than to reply on systems based on consent, i.e. systems under which the passenger's data is obtained with his consent and with no other safeguards. Additionally, the development of potentially 27 national diverging systems for the collection and use of the data would unnecessarily affect the right of privacy of passengers. The Art.29 Working Party on Data Protection, even though not in favour of the use of PNR data, strongly prefer a European instrument with strong data protection guarantees, rather than various diverging national systems with diverging data protection standards.

Another aspect to be taken into account is that the number of travellers is increasing rapidly. This, together with the additional border and security controls that are being put forward by national authorities, have started creating a problem of managing the flows of passengers efficiently. This problem is expected to become worse as the number of travellers grows. Long queues of travellers waiting for security controls may become a terrorist target themselves. The collection and use of PNR data will contribute towards managing this problem more efficiently. The possibility of performing border and security controls of a traveller's PNR data before he or she actually arrives in the country of destination, will provide the possibility of clearing unsuspected travellers and subjecting them only to the absolute minimum controls at the border.

The problem

- Insufficient access of law enforcement authorities to all passenger information for fighting terrorism and organised crime.
- Risk of legal uncertainty for carriers in terms of diverging legal requirements imposed upon them as regards transmission of PNR data and risk of distortion of the internal market through diverging legal requirements.
- Risk of not being able to appropriately manage an ever growing number of travellers and the increase of border and security controls.
- Risk to the protection of citizens' fundamental rights, in particular the right to privacy, if the

exchange of PNR takes place on the basis of incompatible systems.

- Absence of an EU position in this area may hamper an appropriate EU response to the international dimension of the matter and the definition of a global approach to the use of passenger data in the fight against terrorism and organised crime.

2.2. Parties affected by the problem

The problem potentially affects all citizens in the EU, the governments of the Member States as well as the air carriers/operators. Effects may be both direct, in the form of casualties from a terrorist attack, and indirect, in the form of effects on society, economy, and disruption of certain services in case of an attack affecting the provision of such services, as well as affecting their privacy.

- Member States are affected by the problem since they are at a constant risk of a terrorist attack which will affect their citizens and/or their infrastructure. Member States also have to deal with organised crime in its various forms, which affects their societies and economies.
- European citizens are affected since they are at an unpredictable risk of being victims of a terrorist attack, which might result in loss of life, destruction of property, disruption of services. Further, because of the sensitivity of the matter in potentially interfering with the right of privacy of individuals, the potential lack of uniformity in the applicable rules makes it difficult to ensure compliance with the data protection principles.
- Carriers are affected since they face the risk of their means of transport being used in themselves as weapons, and they also face the risk of potential liabilities in case of insufficient controls carried out by them. Further, if each Member State develops its own PNR system, diverging legal requirements might be imposed upon them, putting them in a very difficult position in terms of compliance. As regards the number of flight movements and passengers affected by the possible introduction of PNR measures, air carriers carried approximately 500.000.000 passengers on 3.300.000 flights going in and out of the EU-27 in 2006[5].

2.3. EU right to act

The right of the EU to act in this field is enshrined in Title VI on the Treaty on European Union.

Because of the nature of the terrorist and organised crime threats, investigations carried out by the competent authorities of the Member States are largely dependent on international and trans-border cooperation. It is impossible for the Member States alone to achieve appropriate harmonisation of legal obligations in this area, including the provision of harmonised categories of passenger data, to be imposed on all air carriers operating flights into or from the European Union. In addition, action at the EU level will help to ensure harmonised provisions on safeguarding privacy, whereas if Member States are left to legislate independently, it might be more difficult to achieve harmonisation of such safeguards.

As this issue concerns the security of each individual Member State and of the Union as a whole, the exchange of such information in a harmonised manner is particularly important, especially today where free circulation of persons is a reality in the Schengen area, where there exists an increase in the level of outbound and inbound travellers in the European

[5] Figures according to Eurocontrol on the basis of CFMU IFR Flights.

Union, and where the need for timely identification of possible security threats is greater than ever, while facing the need to appropriately manage an ever-increasing number of travellers.

A further reason for which EU action would be more appropriate is that, the diverging national requirements in this area of Member States which already established similar mechanisms and of the Member States which very possibly would develop such mechanisms in the near future, might trigger negative effects for the economic operators, i.e. the carriers and those authorities having responsibility for the security of citizens in the European Union. It should be noted that the United Kingdom, France and Denmark have already enacted primary legislation and are in the process of enacting secondary legislation through which the PNR data is captured and used for specific purposes, and already it is clear how different such mechanisms are.

In addition, one of the purposes of the use of PNR is to provide competent authorities with the relevant information available in the reservation systems of carriers. Without action at an EU level, carriers might choose to increase their flight activities to those Member States not requiring the provision of passenger information. This could lead to market distortion for transport activities and create an impossible task for the competent border and law enforcement authorities, especially if a legal differentiation on the provision of passenger information would exist between Member States. This could also lead to important security gaps and severely affect the effectiveness of PNR data as a security instrument.

As indicated above, in the absence of EU action, carriers would be faced with diverging legal, technical and financial issues to respond to a multitude of requirements regarding PNR data transfer imposed on them by several States. It has been the aim of the European Union and subsequently of the guidelines of the International Civil Aviation Organisation (ICAO) on PNR to minimise the cost burden on industry. The current report has been elaborated along those lines. One of the major cost-cutting elements is to strictly limit the obligation to provide PNR data to those data elements which are collected by air carriers in their reservation systems as those have been agreed and defined in the ICAO guidelines.

The report will aim to minimise the impact on national public authorities by permitting them to continue using existing control infrastructures. Furthermore the creation of national "Passenger Information Units" or a Centralised EU Unit will provide Member States with a 'single-window' point to obtain the relevant information from the carriers. In particular two or more Member States may establish or designate a common structure to serve as a Passenger Information Unit. As such it will present an economy of scale compared to the current situation whereby the various authorities have to establish individual contacts with carriers and operational infrastructures to deal with the passenger information per department.

On the basis of the above, it can safely be concluded that the EU is both entitled to act and better placed to do so than the Member States.

2.4. Respect of fundamental rights

The proposed measure would aim to prevent and combat terrorism and organised crime. The purpose of such a measure is for the EU to ensure the right of the European citizens to enjoy all their fundamental rights, and especially the right to life and physical integrity.

The proposed actions involve the collection, processing, exchange and use of some personal data of citizens travelling to and from the EU. As such, they might interfere with the right to the protection of private and family life and to the protection of personal data as protected by Art.7 and 8 (subject to the limits set in Article 52) of the Charter on Fundamental Rights of

the European Union and Art.8 of the European Convention of Human Rights. The right to private and family life however is not absolute, but subject to exceptions for reasons necessary "in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others", provided interference is done "in accordance with the law" and is "necessary in a democratic society". As the proposed actions aim to combat terrorism and organised crime, they would clearly come under the umbrella of the exceptions. The proposed proposal would have to ensure that any such interference would be proportionate done "in accordance with the law" and "necessary in a democratic society".

The measure would come under Title VI TEU. Until the time of drafting of the present impact assessment, the Commission Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[6] has not yet been adopted, but it is expected to be adopted shortly.

In view of this, the aim should be to observe the data protection standards as set in European instruments, such as the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe. To that effect, it should be ensured that, to the extent that "sensitive" data[7] are contained in the PNR, they will be filtered out and deleted immediately, that the purpose limitation of the use of PNR data is clearly defined, that the period of retention of the data is limited to the necessary one, that the rights of access, correction and deletion as well as liability provisions are regulated and that the transmissions of the data is sufficiently secure. In practice, all Member States should also already have national legislation in place to cover data processing by law enforcement authorities.

In addition, the competent authorities should be able to use only those PNR elements which are considered necessary for the purposes of the fulfilment of the purpose of the measure, and not all PNR elements. It is suggested that the minimum PNR data elements which should be used are:

Data for all passengers

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name (s)

(5) Address and Contact information (telephone number, e-mail address)

(6) All forms of payment information, including billing address

(7) All travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency /Travel agent

(10) Travel status of passenger including confirmations, check-in status, no show or go show information

---

6 COM(2005) 475.

7 As defined in Article 6 of the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe.

(11) Split/Divided PNR information

(12) General remarks (excluding sensitive information)

(13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any collected API information

(19) All historical changes to the PNR listed in numbers 1 to 18

Additional data for unaccompanied minors under 18 years

(1) Name and gender of child

(2) Age

(3) Language(s) spoken

(4) Name and contact details of guardian on departure and relationship to the child

(5) Name and contact details of guardian on arrival and relationship to the child

(6) Departure and arrival agent

It also important to note that any measure should not oblige carriers to introduce mandatory fields in their collection of PNR from their passengers. The carriers will continue to collect and make available to the competent authorities only those data that are voluntarily given by the passenger for the reservation of his flight, or which have been collected following check-in and boarding.

3. OBJECTIVES

One of the fundamental goals of the European Union is the development of a genuinely European area of justice, freedom and security. Such an area aims to ensure that the fundamental rights of its citizens, such as life, physical integrity and the protection of citizens' personal data and privacy, are guaranteed.

In the Hague programme for 2005-2010, the Council has called again for a common EU approach to the use of passengers' data for law enforcement purposes. A European policy in this area has been announced in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003[8]. The implementation of a genuinely European approach with regard to the use of passenger data for law enforcement purposes should take due account of the following issues:

- The prevention of and fight against terrorism and organised crime,
- The right to privacy and the protection of fundamental rights,
- The security and convenience of passengers,

[8] COM(2003) 826.

- The impact on carriers, in particular in terms of legal certainty and compliance cost,
- The international dimension of this issue,
- The non-distortion of competition.

Such general issues translate into the following operational policy objectives:

- Fighting terrorism and organised crime by using PNR data and protecting citizens' life and physical integrity, the EU as a whole and each Member State,
- Providing legal certainty to carriers in terms of the legal requirements imposed upon them, while avoiding a distortion of the internal market through diverging legal requirements,
- Protecting citizens' fundamental rights, in particular the right to privacy, while recognising the need for a wider sharing of relevant personal data for law enforcement purposes,
- Developing an EU position in this area with the aim to encourage a global approach to the use of passenger data in the fight against terrorism and organised crime.

4. POLICY OPTIONS

The Commission considers that there are two main policy options, which are described below:

4.1. Refraining from addressing the issue at an EU level

This policy option entails no action to be taken by the EU. In effect this means that the issue of exchange of PNR data for the purpose of combating terrorism and organised crime will remain unresolved at an EU level and there will remain only the Council Directive 2004/82/EC[9] on the obligation to carriers to communicate passenger data for the purposes of border control (API data).

This policy option may also entail all or some Member States enacting national legislation obliging carriers to communicate PNR data to the relevant authorities for the purposes of combating terrorism and organised crime or additional purposes. It might also result in some Member States agreeing with third countries to exchange such data with them.

4.2. Introducing a legislative proposal for the use of passenger data for law enforcement purposes

In this policy option, a legislative instrument from the EU would change the current legal situation to ensure that Member States collect, use and share a particular set of passenger data for specific law enforcement purposes, subject to a number of safeguards aimed to provide the highest level of protection of personal data. Such safeguards should be aimed at ensuring the appropriate purpose limitation, defining the period of retention of the data, and setting rules for the security of the data and redress mechanisms.

Such a legislative proposal might take the form of two alternative options which vary in scope, namely:

4.2.1. A proposal covering travel by air with a decentralised collection of the data

Under this policy option, air carriers would be obliged to transmit the PNR data of their passengers to a Passenger Information Unit which would be identified in each

[9] OJ L 261, 6.8.2004, p. 24.

Member State. Such a Unit would process the data and transmit them to the relevant law enforcement authorities.

4.2.2. A proposal covering travel by air with a centralised collection of data

Under this policy option, air carriers would be obliged to transmit the PNR data of their passengers to a Centralised Unit at an EU level. Such Unit would process the data and transmit them to the relevant law enforcement authorities.

Some Member States suggested that the measure should also cover travel by sea and rail. Such an extension of the scope of the measure seems to be premature for the following reasons:

- Currently only air carriers collect such information. The data are given by the passenger voluntarily and are collected and processed by the air carriers for commercial purposes via their Computerised Reservation Systems (CRS). The nature of air travel implies that, as a minimum, the name and flight numbers are known for each passenger at the time that the booking is made. This situation does not exist for most of sea and rail travel. For example, only Eurostar collects some PNR-like data, Thalys collects some data when the reservation is made online and cruise ships collect some PNR-like data. On the other hand, ferries and intercity trains do not collect any data about their passengers and do not have computerised reservation systems which are similar to those of air carriers.
- The setting up of a system to collect such data on such modes of transport would be very costly, both for the carriers but also for the public authorities. The carriers would have to set up the systems of collection, and the public authorities would have to set up the systems for verification of the information, i.e. they would have to install passport control points before boarding a ferry or a train and on arrival. Such changes would involve tremendous costs.
- Such changes would also cause inconvenience to passenger by leading to the extension of time between check-in and departure for such additional modes of transport.
- API data are currently available only for air travel and without such data PNR data are less useful.
- By applying PNR obligations to any other carrier than airlines, considerable costs would arise. They would lead to a multiplication of data collected and processed. Such an extension to sea and rail travel could be considered for the future, once we will have learned from the experiences with PNR collection from air travel.

On the basis of the above, this option is dismissed as from this point and will not be analysed below. The option should be left open to Member States to extend the scope of the proposal to such modes of transport, should they so choose.

The policy option of a legislative proposal would have to include a number of different parameters which would be common for the two alternative options mentioned above. These parameters refer to the geographical scope of the proposal, the purpose and uses of data, the data retention period and possible exceptions to that period, the method of transmission of the data by the carriers, the data to be transmitted from the Unit to the law enforcement authorities and the authorities which will receive such data. An analysis of these parameters is attached hereto as **Annex A.**

5. ANALYSIS OF IMPACTS

The report will try to identify the social and economic impacts of the options, whether direct or indirect, in the short term and in the long term. It should be noted at this stage that no significant environmental impacts could be identified for these policy options. The most significant impacts that have been identified will be analysed below for the following areas: security in the EU, protection of privacy, costs and administrative setup, relations with third countries, competition in the internal market and convenience to passengers.

5.1. Impacts of the option of refraining from addressing the issue at an EU level

This policy option entails no action to be taken by the EU. In effect this means that the issue of exchanging of PNR data for the purpose of combating terrorism and organised crime will not be dealt with at an EU level. The status quo will therefore remain. The status quo, as explained, is that air carriers will be obliged to transmit API data to border control authorities under the Council Directive 2004/82/EC[10] on the obligation to carriers to communicate passenger data (API) for the purpose of combating illegal immigration, and the national measures of the Member States. As analysed above, currently three Member States have relevant legislation. However, the consultations suggested that in the very near future, more and more Member States will start taking such internal measures as well. Therefore, in our assessments, the status quo takes into account the expected developments in the very near future.

- **Security in the EU.** A "no action" policy will hamper the ability of the EU to fight terrorism and organised crime and hence affect European citizens' security. The EU will have less means of identifying when a member of a terrorist organisation or a criminal will be entering their territory and will be left more exposed to terrorist activities. Furthermore, it will deprive the Member States from a very important source of obtaining intelligence allows to establish movements and associations of terrorists and criminals. Moreover, in case that some Member States develop their own systems, terrorists and criminals might choose to enter the EU through a Member State which will not have such a system or have a system of a lower standard. In addition, in view of the free movement of persons within the Schengen area, a system introduced in any Member State might prove to be insufficient, as it cannot go beyond its territory. Furthermore, the security of the EU is the joint responsibility of the Member States and all Member States should act in a harmonised manner in order to achieve results. We do not believe that the aim of increasing the security of the EU can be sufficiently achieved merely by relying on national measures.

    - *Impact on security in the EU: +*

- **Protection of privacy.** The choice of this option would mean that, at an EU level, the right to privacy of the European citizens would not be interfered with at an EU level. Each Member State would have to safeguard the right to privacy of passengers under their own national systems, if such are developed. The development of different legal frameworks and mechanisms to tackle the matter by each Member State might make it more complicated for passengers to be informed and to claim their rights under each national system, but such a complication would not affect the passengers' actual rights. It is indicatory that the joint reply of the Art.29 Working Party on Data Protection was adamant that in the case that Member States commence implementing national measures, then

[10] OJ L 261, 6.8.2004, p. 24.

harmonised EU action would become necessary.

- *Impact on protection of data: 0*

- **Costs on public authorities:** Public authorities in Member States deciding to introduce national PNR legislation would need to set up systems to receive data from carriers. This is anticipated to lead to the development of a number of different national systems of collection and transmission of data, thus having a serious negative impact on efficiency and ultimately on costs, since at the end of the day, each national authority will have to develop technology based systems of transmission to potentially 26 different systems of other Member States. Alternatively, one common system for data exchange connecting to different national systems would also be possible, but could be costly to implement, given expected differences between national systems which might be established.

  - *Impact on costs on public authorities: -*

- **Costs for carriers:** National legislation obliging carriers to communicate PNR data to the relevant national authorities for law enforcement purposes would mean that carriers capturing this data would need to put in place systems ensuring the connection with different national PNR systems. This could create for them substantial financial, legal and technical problems. Considerable costs for carriers can be expected if they would have to respond to multiple, requirements which differ substantially from one another.

  - *Impact on costs for carriers: ---*

- **Relations with third countries:** It is anticipated that more and more third countries will request the provision of PNR data from the EU. In the absence of a joint EU approach in this field, it will become increasingly difficult for the EU to ensure consistency in such bilateral agreements with third countries and to insist on certain standards.

  - *Impact on relations with third countries: -*

- **Competition in the internal market.** In case that some, but not all, Member States choose to develop their own systems of PNR capturing and transmission, carriers operating predominantly from countries which will not have PNR legislation might be in an advantageous position compared to carriers in countries subject to more stringent requirements. This could lead to a distortion of competition in the EU. Requirements differing between countries might also act as a barrier for entering new European markets.

  - *Impact on competition in the internal market: -*

- **Convenience of passengers.** If the EU refrains from taking any action, it is anticipated that, in an effort to increase security, the law enforcement authorities of Member States will increase the checks at border control points, making it increasingly more inconvenient and time-consuming for low-risk passengers to go through passport controls. It is, of course, possible that, Member States which enact national legislation to capture and use

PNR data will not face such a problem, or will face such a problem to a lower extent. However, the decisions of the EU cannot be based on an assumption that all Member States will enact such legislation and that such legislation will cover all relevant points of entry into the EU.

- *Impact on convenience of passengers: -*

5.2. Impacts of the option of introducing a new legislative measure covering air travel with a decentralised collection of data

This policy option entails that air carriers would be obliged to transmit the Passenger Name Record data of their passengers to a Passenger Information Unit which would be designated by each Member State, either directly or through an intermediary, and either filtered out of sensitive and non-required PNR elements or unfiltered of such data. Such Unit would filter when necessary, process the data and transmit them to the relevant law enforcement authorities of its own Member State and to the corresponding units of the other Member States.

- **Security in the EU:** This option would contribute towards a substantial increase of security in the EU since air is the most common means of transport for travelling to and from the EU territory from the vast majority of third countries, and because of its speed, it presents the most attractive means of travel. As a result, even if this measure is limited only to air, a very high percentage of travellers would be covered by it. Further, because of the dramatic effect that an aircraft which crashes has, and because of the destruction that it causes with its crash, it seems to be a preferable means for terrorists, in the case when they seek to use the aircraft itself as a means of performing an act of terror. However, such an option would not cover all controlled border crossings to the EU, and there would continue to be a risk of terrorists and criminals entering its territory via other border crossings. Further, there remains a risk that those wishing to enter the territory of the EU might use alternative means of transport to do so, for example ship, ferry, train, bus, thus making the instrument less effective. Overall, this option could sufficiently achieve the goal of increasing security in the EU. The extension of the scope of the measure to all flights to and from any third country would ensure that the law enforcement authorities are given sufficient tools for identifying when a potential suspect will attempt to enter the territory of the EU and will allow them to establish travel patterns over a given period of time. As regards the decentralised aspect of the collection of the data, this option would potentially entail a faster transmission of the captured PNR data from a Passenger Information Unit which would be identified in each Member State to the relevant competent law enforcement authorities, than under the Centralised Unit option. Such faster transmission is important since it allows more time to process the data and identify the high-risk passengers, especially in cases in which tickets for travel were bought at the last minute. Such option would thus contribute to increasing security in the EU quite substantially. There is a risk, however that the Passenger Information Units of the Member States apply diverging criteria in assessing high-risk passengers, in which case there might be risks of high risk passengers entering the Union unidentified.

- *Impact on security in the EU: ++*

- **Protection of privacy:** This option would involve the capturing and processing of the data of only air passengers. This would contribute towards minimising the interference with the passengers' right to privacy. As regards the decentralised aspect of the collection of the data, the bulk of the transmitted data would remain within one Member State and only the PNR data of identified high-risk passengers would be transmitted to other Member States. This would involve less interference with the right to privacy of passengers, making it more likely for such inference to be deemed proportionate. Provision will be made to ensure that sensitive data are filtered out and deleted either by the receiving national authority or an intermediary which the carrier appoints for this purpose, and other data protections safeguards will be ensured, i.e. rights of access and correction, limited periods of retention, measures to safeguard data security, clear purpose limitations.

    - *Impact on protection of privacy: ++*

- **Costs on public authorities:** The costs for establishing the system would admittedly be substantial for the Member States since each Member State would have to set up or identify a Passenger Information Unit which would receive the data and would have to develop the necessary mechanisms for the filtering and processing of the data and their transmission to the relevant law enforcement authorities and the Passenger Information Units of the other Member States. The operation of such a Unit is estimated to require between 30-50 members of staff for Member States with few international flights and 70-100 for Member States with many international flights. Since the setting-up and operation of such a Unit will involve substantial costs, there should be a possibility of two or more Member States establishing or designating the same Passenger Information Unit to receive, filter, process and forward the data. This option would be especially helpful to Member States which have few international flights or which do not face a severe threat to their security or intense problems with organised crime.

    - Impact on costs on public authorities: --

- **Costs on carriers:** Air carriers are the only providers of transport services that already have mechanisms with which to capture the PNR data of passengers. These mechanisms were developed and are used for commercial purposes. Other types of carriers would have to set up such mechanisms from scratch and change their operational systems substantially. This option would not therefore entail quite substantial costs and administrative changes for the carriers. Carriers would have to bear the cost of "pushing" the data to the Passenger Information Unit, which is estimated at around 0,04 Euro per passenger, or the cost of "pulling" data which is estimated at around 0,03 Euro per passenger The carriers will also have to bear the cost of setting-up the system (hardware and software) which is non-recurring, as well as personnel and maintenance costs, which are recurring costs.

    - *Impact on costs on carriers: --*

- **Relations with third countries:** It is anticipated that more and more third countries will request the provision of PNR data from the EU. This option 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 the possibility of requesting reciprocal treatment from third countries with which the EU has an agreement, something that is not possible today. Since the proposed measure will request specific action from non-EU carriers, there is a possibility that the third countries in which such carriers are based will introduce similar measures or refuse to provide such data unless bilateral agreements are concluded with the EU as retaliatory actions. Even though such retaliatory actions from third countries are possible from a legal and a practical point of view, it is not anticipated that they will occur. This is based on our experience with the US, Canadian, Australian and New Zealand national measures. This experience shows quite clearly that, despite such national measures which affect carriers worldwide, only the EU has refused to permit its carriers to provide such data unless there were special agreements to that effect. This is probably based on the very high data protection standards that exist in the EU. Additionally, the setting up and operation of a PNR system requires a high investment by the country that introduces it which can be a dissuasive factor for most third countries. Therefore, our consultations and experience shows that the possibility of retaliatory action by third countries does not present such a great risk as to outweigh the advantages that the proposed measure offers to security.

  - Relations with third countries: +

- **Competition in the internal market:** The distinction between air and other forms of travel bears a risk, albeit a minor one, that air carriers might be put at a competitive disadvantage as they would have to incur expenses for complying with the system that non-air will not have. This might lead to a distortion of competition in the EU. However, this would depend on which routes are considered to be in competition with other routes, and which markets are considered separate. As regards the decentralised aspect of the collection of the data, it is not foreseen that this option would have any significant impact on competition in the internal market.

  - Impact on competition in the internal market: -

- **Convenience of passengers:** This option would contribute towards increasing the convenience of air passengers, because it would minimise checks at border control for air passengers and make it more convenient and quick to go through such checks. The reason for this is that, the transmission of PNR data to the receiving Member State before the passengers actually arrive makes it possible for the border control authorities to identify the passengers who seem to present a high risk to the receiving State. As a result, it will become possible for all other passengers to be subjected only to minimum border controls and therefore limit the time required to go through such controls. This option would therefore contribute towards achieving great convenience for legitimate passengers. As regards the decentralised aspect of the collection of the data, it is not foreseen that this option would have any significant impact on passenger convenience.

  - *Impact on the convenience of passengers: ++*

5.3. Impacts of the option of introducing a new legislative measure covering air travel with a centralised collection of data

This policy option entails that air carriers would be obliged to transmit the Passenger Name Record data of their passengers to a Centralised Unit at an EU level, either directly or through an intermediary, and either filtered out of sensitive data and non-required PNR elements, or unfiltered of such elements. Such Unit would filter when necessary, process the data and transmit them to the relevant law enforcement authorities of the Member States. One of the existing bodies and agencies of the EU could serve as such a Centralised Unit, and it would not be necessary to create a new body. Europol could be the most suitable under the circumstances, to perform the functions of the Centralised Unit.

- **Security in the EU:** This option would contribute towards a substantial increase of security in the EU since air is the most common means of transport for travelling to and from the EU territory from the vast majority of third countries, and because of its speed, it presents the most attractive means of travel. As a result, even if this measure is limited only to air, a very high percentage of travellers would be covered by it. However, such an option would not cover all controlled border crossings to the EU, and there would continue to be a risk of terrorists and criminals entering its territory via other border crossings. Further, there remains a risk that those wishing to enter the territory of the EU might use alternative means of transport to do so, for example ship, ferry, train, bus, thus making the instrument less effective. Overall, this option would sufficiently achieve the goal of increasing security in the EU. The extension of the scope of the measure to all flights to and from any Member State would ensure that the law enforcement authorities are given sufficient tools for identifying when a potential suspect will attempt to enter the territory of the EU. As regards the centralised aspect of the collection of the data, this option would ensure the application of common criteria for identification of high-risk passengers and would provide the possibility of identifying travel patterns and behavioural characteristics more accurately because they would be based on PNR data for the whole of the EU. As such, it would be expected that the option of a centralised collection of data would contribute substantially to increasing security in the EU. However, for the purpose of performing the risk assessment of the passengers, the responsible central authority would have to gather intelligence and information from all the Member States. Such intelligence will have to be current at all times, and the processing system will have to be fed with information almost every day. In addition, the responsible authority would have to have direct access to a variety of different national databases in order to be able to carry out the risk assessments. Such direct access is considered by the Member States to be highly sensitive and the consultations with the Member States indicated that they would be very reluctant to exchange such information and give such direct access. This reluctance would mean that such an option would bear a high probability of failure and would not able to work well in reality. This is expected to hamper substantially the positive impact that the measure is expected to have on security.

    - *Impact on security in the EU: +*

- **Protection of privacy:** This option would involve the capturing and processing of the data of only air passengers. This would contribute towards minimising the interference with the passengers' right to privacy. As regards the centralised aspect of the collection of the data, the advantage is that an EU Centralised Unit might be in a better position to ensure that the data is transmitted and used with adequate and uniform safeguards and redress mechanisms

for the data subjects. This might ultimately involve less interference with the right to privacy of passengers, making it more likely for such inference to be deemed proportionate. Such Unit would also ensure that sensitive data are filtered out and deleted , and other data protections safeguards will be ensured, i.e. rights of access and correction, limited periods of retention, measures to safeguard data security, clear purpose limitations.

- *Impact on the protection of privacy: ++*

- **Costs on public authorities:** The costs for establishing the system would admittedly be substantial. Such costs would be borne by the EU budget and each Member State separately would not have to bear any costs since they would not have to develop their own Passenger Information Unit. However, the costs of setting up the EU Centralised Unit would be very high since such a Unit would have receive the data and develop the necessary mechanisms for the processing of the data and their transmission to the relevant law enforcement authorities. The mechanism which would have to be developed would have to be of an especially high capacity in order to deal with the vast amounts of data from carriers and would have to be quite complicated. Such a system might run a risk of being subject to frequent crashes because of the vast traffic of data, with a risk of being unworkable. A centralised system can be distinguished from systems such as SIS and VIS since the traffic of data which will be put in such a system will be substantially more than those in SIS and VIS. SIS and VIS contain the data of specified individuals which are put into the systems by each Member State. On the contrary, the Passenger Name Record data which will have to be handled by such a Centralised Unit would relate to approximately 500.000.000 passengers who fly in and out of the EU every year. Such figures are also expected to rise every year.

  - *Impact on costs on public authorities: --*

- **Costs on carriers:** Air carriers are the only providers of transport services that already have mechanisms with which to capture the PNR data of passengers. These mechanisms were developed and are used for commercial purposes. Other types of carriers would have to set up such mechanisms from scratch and change their operational systems substantially. This option would not therefore entail substantial costs and administrative changes for the carriers. Carriers would have to bear the cost of "pushing" the data to the Centralised Unit, which is estimated at around 0,04 Euro per passenger,, or the cost of "pulling" data which is estimated at around 0,03 Euro per passenger, Carriers will also have to bear the cost of setting-up the system for "pushing" or "pulling" (hardware and software) which is a non-recurring cost, as well personnel and maintenance costs which are recurring costs.

  - *Impact on costs on carriers: --*

- **Relations with third countries:** It is anticipated that more and more third countries will request the provision of PNR data from the EU. The proposed measure 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 the possibility of requesting reciprocal treatment from third countries with which the EU has an agreement, something that is not possible today. Since the proposed measure will request specific action from non-EU

carriers, there is a possibility that the third countries in which such carriers are based will introduce similar measures or refuse to provide such data unless bilateral agreements are concluded with the EU as retaliatory actions. Even though such retaliatory actions from third countries are possible from a legal and a practical point of view, it is not anticipated that they will occur. This is based on our experience with the US, Canadian, Australian and New Zealand national measures. Such experience shows quite clearly that, despite such national measures which affect carriers worldwide, only the EU has refused to permit its carriers to provide such data unless there were special agreements to that effect. This is probably based on the very high data protection standards that exist in the EU. Additionally, the setting up and operation of a PNR system requires a high investment by the country that introduces it which can be a dissuasive factor for most third countries. Therefore, our consultations and experience shows that the possibility of retaliatory action by third countries does not present such a great risk as to outweigh the advantages that the proposed measure offers to security.

- *Relations with third countries: +*

- **Competition in the internal market:** The distinction between air and other forms of travel bears a risk, albeit a minor one, that air carriers might be put at a competitive disadvantage as they would have to incur expenses for complying with the system that the carriers who provide other types of transport services will not have. This might lead to a distortion of competition in the EU. However, this would depend on which routes are considered to be in competition with other routes, and which markets are considered separate. As regards the centralised aspect of the collection of the data, it is not foreseen that this option would have any significant impact on competition in the internal market.

  - *Impact on competition in the internal market: -*

- **Convenience of passengers:** This option would contribute towards increasing the convenience of air passengers, because it would minimise checks at border control for air passengers and make it more convenient and quick to go through such checks. The reason for this is that, the transmission of PNR data to the receiving Member State before the passengers actually arrive makes it possible for the border control authorities to identify the passengers who seem to present a high risk to the receiving State. As a result, it will become possible for all other passengers to be subjected only to minimum border controls and therefore limit the time required to go through such controls. This option would therefore contribute towards achieving great convenience for legitimate passengers. As regards the decentralised aspect of the collection of the data, it is not foreseen that this option would have any significant impact on passenger convenience.

  - *Impact on the convenience of passengers: ++*

6. COMPARING THE OPTIONS

The "no action" policy option does not present any real strength in improving security in the EU. On the contrary, it is anticipated that, bearing in mind the way that this field is currently developing, it will have negative impacts in the sense of creating administrative difficulties stemming from numerous diverging systems, increased costs of compliance with such

diverging systems and distorting competition. The costs of compliance with potentially 27 diverging systems would be enormous both for the public authorities and the carriers. The development of different legal frameworks and mechanisms to tackle the matter by each Member State would bear more risks of leaving the citizens exposed to more threats to their privacy. It would be more difficult to ensure that the data protection principles are followed under each such diverging system.

The legislative proposal policy option possesses the clear advantage of increasing security in the form of reducing the risk of terrorist attacks and of organised crime being committed on the territory of the EU. It presents further advantages in the form of preventing the distortion of competition by imposing the same requirements for all carriers which operate flights to and from the EU. The costs for the carriers and the administrative setup would ultimately be much less than in case that the Member States develop their own systems. The convenience to passengers would increase, thus minimising the time required for border control for all unsuspected passengers. Finally, this policy option would provide harmonisation of the various aspects of the systems for the exchange and use of PNR and of the safeguards given to passengers aimed to protect their right to privacy.

Between the "no action" policy and the legislative proposal policy, the legislative proposal presents clear advantages.

Between the two options for a legislative proposal, the option of a decentralised collection of data presents advantages over the centralised option in relation to the increase to the security of the EU. The option of a centralised collection of data would have a high risk of failure both on a political level because of failure to ensure adequate co-operation between the Member States, and on a practical level because of failure of the system to be operable and reliable.

Synopsis of the impacts of the policy options

Table of symbols (distinguishes between (-) for negative impact and (+) for positive)

Table of symbols	
Small impact	- / +
Medium impact	-- / ++
Significant impact	- - - / +++
No impact	0

Summary table

Policy option	**Increased security**	**Increased convenience to passengers**	**Relations with third countries**	**Protection of privacy**	**Impact on Competition**	**Costs on carriers**	**Costs on public authorities**
No action by EU	+	-	-	**0**	-	---	-
Legislative proposal covering travel by air with decentralised collection of data	++	++	+	++	-	--	--
Legislative proposal covering travel by air with centralised collection of data	+	++	+	++	-	--	--

7. PREFERRED POLICY OPTION

On the basis of the above, the creation of a new legislative proposal applicable to travel by air with a decentralised collection of data seems to be the best policy option. This option would be preferable since it would provide better means of increasing security in the EU, while at the same time ensuring the better protection of data and minimising the costs for its setup and operation. It should be noted that it is not believed that this option presents the ultimate solution to the problem but, at the current stage, it is the most feasible solution. It presents a good starting point and will help towards gathering experience in this very new field. It is foreseen that this proposal will be evaluated and, if possible, extended to a wider application at a later stage. It should be left up to the Member States to extend the scope of such proposal to other modes of transport at this point. Further, Member States should be able to conclude bilateral or multilateral agreements or arrangements for the purpose of enhancing or facilitating the provisions of such proposal.

The EU needs to act as soon as possible in this area in order to decrease/minimise the chance of various incompatible systems being developed by each Member State. Different approaches by different Member States would lead to inconsistencies, uncertainty and different rights for individuals, which would entail citizen dissatisfaction as well as high costs for implementation and compliance.

It might be argued that, since the PNR data are initially captured by the carriers in the course of a commercial activity, namely the sale of travel ticket and the provision of a service, the measure could be adopted under community law. However, according to the judgement of the European Court of Justice of 30/5/2006 in joined cases C-317/04 and C-318/04[11], it is important to take into account the reason for which the captured data will be transmitted, in order to decide on the legal basis of a legislative proposal. In the current case, the transmission of the data would be made for the clear purpose of improving access to information for the purpose of combating terrorism and organised crime. Therefore, the proposal should most suitably take the form of a Framework Decision under Title VI of the Treaty on European Union.

Costs of preferred option

An analysis of the costs of the preferred policy option appear in detail in **Annex C.** Such costs are differentiated between costs for public authorities and costs for carriers.

In relation to public authorities, the estimated costs for all Member States together are:

Setting-up cost (non-recurring cost)	614,833,187 Euro
BUT assuming an amortisation period of five years	122,966,637 Euro
Annual personnel costs (recurring)	11,686,749 Euro
Annual maintenance costs (recurring)	61,483,319 Euro
In relation to all EU carriers together, such costs are:	
Setting-up cost for PUSH (non-recurring costs)	11,647,116 Euro
BUT assuming an amortisation period of five years	2,329,423 Euro

[11] European Court Reports 2006, page I-04721.

Transmission costs PUSH twice per passenger (recurring)	2,250,080 Euro
Personnel and maintenance costs (recurring)	5,435,321 Euro

8. MONITORING AND EVALUATION

It is important that the proposal includes provisions for its monitoring and evaluation. Such arrangements could be:

- Each Member State could prepare and annual report on the implementation of the systems containing information on the volumes of data received, the cases which have ended in successful identifications of suspects and the cases in which data received were used towards a criminal or intelligence investigation.
- The setting up of a group of experts of each Member States by the Commission for the development of the common protocol or encryption standards. This may be done between the adoption of the legislative measure and its coming into force.
- The Commission could review the operation of the Framework Decision after five years from its entry into force and submit a report to the Council.
- The Commission could prepare an assessment on the possibility of extending the measure to sea and rail travel if and when the API Directive is amended to that effect as well. This would provide the opportunity to have a transitional period and to gain experience from the functioning of the PNR gathering for air travel, before extending it to other modes of travel.

ANNEX A – ANALYSIS OF OTHER PARAMETERS

The preferred policy option entails the Commission initiating a legislative proposal for a Framework Decision which would create an obligation on air carriers to transmit the PNR data to Passenger Information Unit which would be established in each Member State.

This policy option, as well as any other option based on a legislative measure, has a series of other parameters which complement the measure. The Member States and other organisations as mentioned in the Report were consulted on these parameters and the synopsis of the results appear in Annex B. This Annex is based on a preliminary analysis of these parameters.

Modes of transport

The options available are to limit the effect of the measure to (i) air carriers, (ii) air and sea carriers, or (iii) air, sea and rail carriers.

As a first step, it seems more proportionate that the proposal is limited to air carriers. Such a limitation would challenge the effectiveness of the measure in relation to increasing security in the EU. However, the costs and administrative adaptations which would be involved in the development of mechanisms for the capturing of PNR data by non-air carriers would be so high, at this stage, as to outweigh the disadvantages to security. Further, the costs of running the system would also be much more costly in case of extension of the measure to other modes of transport, since the volume of the data which will be involved will be much higher than if only air data are involved.

Even though this might not use the full potential of the measure, it appears to be the most feasible currently, especially in view of the fact that API data are at present collected only for air carriers. It might be useful, however, to consider extending the ambit of this proposal to sea and rail travel. This may be done by foreseeing a review of this proposal in five years, and taking that opportunity to assess the viability of such an extension.

Geographical scope

The options available are to limit the effect of the measure to (i) travel from a third country to a Member State, (ii) and from a Member State to a third country, or (iii)… and from a Member State to a Member State.

It would seem inadequate to choose to apply this proposal only to travel from a third country to a Member State. Such a choice would give only a limited input towards the sought goal of increasing security and providing a tool to fighting terrorism and organised crime, because the competent authorities would not be able to establish travel patterns and behavioural characteristics sufficiently without the data for outgoing flights as well

The option of making the instrument applicable to all travel, including intra community and internal travel, would might be considered disproportionate to the objective sought. The first reason is political, because to do so would in effect reintroduce border controls within the EU, as in order to identify a high-risk passenger upon his/her entry into one Member State, the passports of all passengers would have to be read as for third country nationals. This might have a serious effect on the way of travel that EU citizens are now used it in the EU and it would create serious inconvenience for the passengers who would have to be reintroduced to long queues at passport controls. Furthermore, API data is currently only required for international flights. (API Directive

2004/82/EC), and without the existence of API data, PNR data cannot fulfil its full potential. Additionally, the very large numbers of travellers on intra-EU flights would mean that the costs for setting up and operating the system would be much higher. The hardware and software that will be required to set up the system would have to have a much larger capacity, and thus be much more expensive. According to our analysis and our consultations with stakeholders, such increased costs would outweigh the benefit of the measure.

The most reasonable and proportionate option at this stage would be to extend the measure to travel from a third country to a Member State and from a Member State to a third country. This option would provide a substantial input towards the purpose of the instrument, while not presenting serious negative impacts. The risk to distortion of competition would not outweigh the benefits to security under this option. It should be mentioned that this option is foreseen to include also connecting flights via a Member State, i.e. flights commencing from a third country, and connecting to one Member State via another Member State, using the same ticket.

Purpose and use of the data

The options are to limit the purpose and use of the data for (i) preventing and fighting terrorism and related offences, (ii) … and other serious crimes, including organised crime, or (iii) … and other more general policy options.

The limitation of the purpose and use of the data to the fight against terrorism would seem to miss the full potential of this proposal without adding any strong advantages to it. More specifically, the advantage to the protection of privacy of passengers would outweigh the disadvantage to security.

On the other hand, the extension of the scope of the proposal to other, more general, policy options, would seem quite interesting, especially as regards the use of the data in the fight against illegal immigration and as regards less serious crimes. Such a step however is premature, and the need to use PNR data for such policy options is not as clear and direct.

The option of extending the scope of the instrument to the fight against terrorism and organised crime would seem to be the most proportionate and appropriate. The definition of what constitutes a terrorist offence could be taken from the Framework Decision on combating terrorism 2002/475/JHA[12] and the Council of Europe Convention on the Prevention of terrorism of 2005. However, it is important that care is taken in the definition of "organised" crime. The definition of "organised" crime could be taken from the Council Framework Decision on the fight against organised crime (xx/xx).

Data retention period

The options are to delete the data from the databases of the Passenger Information Units (i) upon arrival at the country of destination or (ii) after longer periods.

The option of deleting the data upon the arrival of the passengers at the country of destination seems to be insufficient for ensuring an adequate level of security and would miss the potential of PNR as an instrument. Even though such a period of retention was deemed adequate for the purposes of tackling illegal immigration under Council directive 2004/82/EC, the objectives

[12] OJ L 164, 22.6.2002, p. 3.

sought by that Directive, i.e. border control, are very different in nature from the objectives of the current Directive, which are more complex in nature. For example, it would be impossible to develop the risk-assessment mechanisms and behavioural patterns if the data would be deleted immediately. Also, in case that a person is identified as a criminal or a terrorist after the flight has landed, it would be impossible to find the persons with whom he was flying.

It would seem clear that a longer period of retention of the data is needed. The question of how long this period should be, is one that depends on what would be deemed proportionate. Obviously, the longer the data is retained for, the better it is for the purposes of the law enforcement authorities. For the purposes of this report, the period of 5 years is proposed for the retention of the data in an active database. This proposal was the result of our consultations with the Member States and of experience gained from international agreements that the EU signed in the field. This period was deemed as striking an acceptable balance between what the law enforcement authorities wanted and what is considered adequate and acceptable. Any period which is chosen however, must be fixed so as to ensure legal certainty for the carriers and the Passenger Information Units and to meet data protection requirements. It would not be advisable to adopt a minimum and maximum period, and leave it to the Member States to decide which to adopt. All authorities and bodies involved in the capturing and exchange of the PNR data should keep them for the same period, no matter for whom they are keeping them.

This proposal further proposes that, upon the expiry of the five year period of retention of the data, such data are transferred to a dormant database and kept there for a period of eight years. During such eight years, the data should be accessed, processed and used only with the approval of the responsible Minister and only in exceptional circumstances in response to a specific case, threat or risk.

Exceptions to the period of retention

The options are to (i) not have any exceptions to the above periods of retention, or (ii) allowing exceptions to the period of retention of the data is being used for a crime investigation or intelligence operation.

The option of not having any exceptions to the period of retention of data seems to be disproportionately inflexible in comparison to the advantages that this option carries with it. More specifically, the obstacles that such an option would pose to law enforcement, in the form of time restraints to investigating and prosecuting a crime, would be substantial.

On the basis of the above, it seems clear that the period of retention should be subject to exceptions. Such exceptions could be situations in which there is an ongoing criminal or intelligence operation. The exceptions should be valid for active and dormant data retention periods.

Body receiving the data from the carriers

The options are that the data is received from the carriers by (i) a Passenger Information Unit to be established in each member State, or (ii) a Centralised EU Unit.

An important impact of the choice between the two options relates to the political and technical feasibility of the system.. The option of creating Passenger Information Units in each Member State would entail costs which will be borne by each Member State directly. The costs would need to cover the creation of the Unit, its staff, the development of the mechanism for the

processing of the data and their transmission to the competent authorities. Such costs are not foreseen to be enormous since the mechanisms would not need to be particularly complex, as can be seen in Annex C. In the case of creation of a Centralised EU Unit, its costs would be borne by the EU budget. Such costs are foreseen to be much greater than the first option since the mechanisms would have to be much more complex. It would be suggested that one of the existing agencies of the EU acts as such a Centralised Unit. In this way, it would not be necessary to create another body, hence reducing substantially the amount of costs which will be required. In general, it could be foreseen that the ultimate total costs of the first option would be more than the second option.

An effective Centralised EU Unit would also present advantages to increasing security, to applying uniform standards of identification of suspects everywhere in the EU and for ensuring adequate protection of data. However, for the purpose of performing the risk assessment of the passengers, the responsible central authority would have to gather intelligence and information from all the Member States. Such intelligence will have to be current at all times, and the processing system will have to be fed with information almost every day. In addition, the responsible authority would have to have direct access to a variety of different national databases in order to be able to carry out the risk assessments. Such information is considered by the Member States to be highly sensitive and the consultations with the Member States indicated that they would be very reluctant to exchange such information and give such direct access. Such reluctance would mean that such an option would bear a high probability of failure and would not able to work well in reality. This is expected to hamper substantially the positive impact that the measure is expected to have on security.

Finally, on the basis of all the above, it seems that the option of the national Passenger Information Units would be preferable because of the fact that the data will be used and shared with fewer authorities and entities than under the Centralised Unit. The data would also be accessible by fewer individuals and authorities. Since the setting-up and operation of such a Unit will involve substantial costs, there should be a possibility of two or more Member States establishing or designating the same Passenger Information Unit to receive, filter, process and forward the data. This option would be especially helpful to Member States with few international flights or which do not face a severe threat to their security or considerable problems with organised crime.

Method of transmission of the data by the carriers

The options are that the data is transmitted by (i) "push", (ii) "pull", or (iii) a combination of these.

'Push' is the method under which carriers transmit ("push") the required Passenger Name Record data into the database of the authority requesting them, whereas "Pull" is the method under which the authority requiring the data can reach into ("access") the carrier's reservation system and extract ("pull") a copy of the required data into their database.

The advantages of the "push" system over the "pull" system are undisputable. The risks to the protection of the data of passengers when using the "pull" system are so high as to outweigh the advantage that it offers on costs. The risks of the "pull" system are that the authority which receives the data will be able to access all data in the reservation systems of the carriers and

would then have to filter them out themselves. The carriers are left therefore with no control as to what happens to the data which they have collected and for which they are responsible.

Furthermore, "push" systems are currently being developed and finalised in Europe and will most probably be available before a potential framework decision is adopted.

Nevertheless, in case of carriers that do not yet have the technology to "push", or that do not wish to bear the costs of "pushing", or that do not object to "pull", the Passenger Information Units of the Member States might have to "pull". It is intended that as a general rule, EU carriers will be obliged to use the "push" method and Passenger Information Units should make every effort to receive data by "push" before resorting to "pull" as regards non-EU carriers.

Carriers may also choose to transmit the data to the Passenger Information Units through a designated intermediary which can be an independent entity. Such entity will be contracted by the carrier to receive the data from it and to transmit them to the relevant Passenger Information Unit. Carriers may also authorise intermediaries to filter the data before transmitting them to the Units. Such intermediaries will be obliged to use the "push" method for transmitting data to the Units and they shall be deemed to be acting on behalf or as representatives of the carriers. The databases of intermediaries will have to be held in the EU.

Data to be transmitted from the Passenger Information Units to the competent authorities

The options are that the data is transmitted (i) in bulk, or (ii) on a case-by-case basis

The advantage to the increase of security in the case of bulk transmissions of data is minor and does not outweigh the disadvantage on the protection of data.

It seems preferable that there is a filtering of the data which will be transmitted to the competent law enforcement authorities. And this filtering could best done by the Passenger Information Units of the Member States or the EU Centralised Unit (depending on which option is finally adopted). This would mean that the Passenger Information Unit or Centralised Unit will run the PNR data through the alert systems, the special intelligence and the risk-assessment systems and will identify the "high-risk passengers". Then the Units will send only the PNR data of such passengers to the law enforcement authorities. Such law enforcement authorities will not have access to the PNR data of unsuspected/legitimate passengers. This way, the costs of this exercise would be borne by the Member States or the EU budget, and further, the risk of abuses to the protection of the data of unsuspected passengers would be minimised.

In addition, there is an added value in permitting the Passenger Information Unit or any of the designated competent authorities of a Member State to request the Passenger Information Unit of any other Member State to provide it with specific data which are kept in the latter's active or inactive database subject to different rules. The request may be based on any one or a combination of data elements.

Bodies receiving data from the Passenger Information Units

The options are that the data is transmitted by the Passenger Information Units to (i) only the national competent law enforcement authorities of the country of destination/departure, (ii)… and to national competent law enforcement authorities of other member States, or (iii)… and to competent authorities of third countries which satisfy certain criteria.

The Passenger Information Units should perform the filtering and the risk-assessment and then send to the competent national law enforcement authorities of the country of destination/departure only the PNR data of the identified high-risk passengers. The Passenger Information Units should also send the PNR data of the identified passengers to the Passenger Information Units of the other Member States, which should then, in their turn, transmit them to their competent national law enforcement authorities. The possibility of sending the PNR data of identified high-risk passengers to the competent authorities of third countries should be the prerogative of the Member State which performs the filtering, whereas a Member State which is merely the recipient of such data should not be able to transmit them to a third country.

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 Passenger Information Units according to the normal practice under the current measure. The Passenger Information Unit which receives such data shall transmit them to the competent authority of the third country with which such an agreement exists.

The choice of this option seems to offer the best balance between ensuring security and protecting the data of passengers.

Summary table on impacts of parameters of preferred option

Table of symbols ***(distinguishes between (-) for negative impact and (+) for positive)***

Table of symbols	
Small impact	- / +
Medium impact	-- / ++
Significant impact	- - - / +++
No impact	0

Policy option	**Increased security**	**Increased convenience to passengers**	**Protection of privacy**	**Impact on Competition**	**Costs for Business**	**Costs for public authorities**
Modes of transport						
Air	++	++	-	-	-	-
Air and sea	+++	+	-	-	--	--
Air, sea, rail	+++	-	--	**0**	---	---
Geographical						

scope						
From third country to MS	+	+	-	--	-	--
… and from MS to third country	++	++	--	--	--	--
… and from MS to MS	+++	+	---	**0**	---	---
Purpose and use of data						
Fight and prevent of terrorism and related crimes	++	++	-	**0**	-	-
… and other transnational organised crime	+++	++	--	**0**	-	-
…and other policy objectives	+++	-	---	**0**	-	-
Data retention period						
Delete after arrival at destination	+	**0**	+++	**0**	**0**	+
Delete after 3.5 years	++	**0**	-	**0**	**0**	-
Delete after longer periods	+++	**0**	---	**0**	**0**	---
Exceptions to data retention periods						
No exceptions	-	**0**	++	**0**	**0**	**0**
Exceptions when used for crime investigation/ intelligence operation	+++	**0**	--	**0**	**0**	**0**
Body receiving data from carriers						

Passenger Information Unit in MS	+++	**0**	+++	**0**	**0**	+++
Centralised EU Unit	+++	**0**	++	**0**	**0**	+++
Method of transmission of data by carriers						
"Push"	**0**	**0**	+++	**0**	--	--
"Pull"	**0**	**0**	---	**0**	--	--
Data to be transmitted from PIU to national authorities						
In bulk	+	**0**	--	**0**	+	-
On case-by-case basis	+	**0**	++	**0**	+	--
Bodies receiving data from PIU						
National competent authorities	++	**0**	-	**0**	-	-
…and authorities of other MS	+++	**0**	--	**0**	-	--
…and authorities of third countries	+++	**0**	---	**0**	-	---

ANNEX B – TABLE OF REPLIES TO THE QUESTIONNAIRE

Replies from MS on the questionnaire

"A common approach to the use of PNR Data for law enforcement purposes"

	AT	BE	BU	CY	CZ	DA	DE	EL	ES	ET	FR	HU	IT	LT	LV	LU	NL	PL	PT	RO	SL	SK	SV	UK
Policy Option 1: Nothing 2: Legal instrument 3: Encourage Cooperation	1	2	2	2	2	2	2	2	2	2	2	1	2	2	2	**2**	General remarks	2	2	2	2	2	3	2
Scope (forms of transport): 1:Air 2: Air and sea 3: Air, sea and rail	1	1 (1 st step)	3	2	1 (1st step)	1	2	1	3	2	3 (progressively)	1	2	1 (1st step)	3	**3**	1	1	1(ev.2)	1	2	1		3
Scope (geographic): 1 : From third country to MS 2: ... and from MS to third country 3: ... and from MS to MS	2	2 (1st step)	3	3	1 (1st step)	2	3	2	2	3	2 (maybe even 3)	2	2	2	2		2	2	2	3	2	2		3
Use/Purpose of collecting PNR data: 1 : Preventing and fighting terrorism and related crimes 2: ...and other transnational, serious, organised crimes 3: ... and more general public policy purposes	2	2	2	2	2 (maybe 3 as next step)		2	2	2	2	2 plus illegal immigration minus social and fiscal crimes	2	2	2	2			2	2	2	2	2		3
Data retention period: 1 : delete on arrival in destination country 2: delete after 3.5 years from transfer date 3: delete after longer period		2	2	2	2	1 year	2	2	2	2	3(5 years)	2	2	2	2			2	2	2	2	2?		2
Exceptions 1: None 2: Where used for crime investigation/intelligence operation	1	2	2	2	2		2	2	2	1	2	2	2	2	2			2	1?	2	2	2		2
Body receiving PNR data 1: Passenger Information Unit in MS 2: Centralised System	2	1	2	2	2		1	1	1	1		1	1	1	1	2			1	1	2	1		1
Method of transmitting PNR data 1: Push Method 2: Pull Method 3: Hybrid	2	1		1	evaluate	1	1	1	1	1 or 3	1	1	1	1	1	1		1	1	1	2			combine
Bulk or case by case transfers 1: Bulk 2: Case by case	2	combine		2	evaluate	2	2	2	1	1		2	2	2	2				2	2	2	Rather 1		combine

Onward Transfer of PNR data 1 : Only to national competent authorities 2: ... and other MS's competent authorities 3: ... and third countries' competent authorities	1	3	3	2	3			2	1	2 option 3 if mutual agree me		2	3	3	2				3	3	2			3
Security Data 1 : Specify common encryption levels 2: Require common transmission protocols	both		1	1	evaluate		1	2	combin e	combin e	1	2	2	2	evaluat e				combi ne	2	1			evaluat e

ANNEX C – TABLE OF ECONOMIC IMPACTS OF PREFERRED OPTION

Proposal On A Common Approach to the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes If the act assessed is the transposition of an act adopted at another level, insert here the name and reference of that 'original' act						Tariff (€ per hour)		Time (hour)		Price (per action or equip)	Freq (per year)	Nbr of entities	Total nbr of actions	Total cost	Regulatory origin (%)			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group	i	e	i	e						Int	EU	Nat	Reg
1			Submission of (recurring) reports	Submitting the information (sending it to the designated recipient)	non-recurrent costs for airlines (installation of IT systems and software)					2.329.423,00	1	1	1	2.329.423		100%		
2			Submission of (recurring) reports	Adjusting existing data	recurrent costs for airlines (personnel and operation of the system)					5.435.320,94	1	1	1	5.435.321		100%		
			Submission of (recurring) reports	Submitting the information (sending it to the designated recipient)	recurrent costs for airlines (transmission of PNR data)					0,04	1	1	54.880.000	2.250.080				
3			Other	Inspecting and checking (including assistance to inspection by public authorities)	non-recurrent costs for public administrations (installation of IT systems and software)					122.966.637,04	1	1	1	122.966.637		100%		
4			Other	Inspecting and checking (including assistance to inspection by public authorities)	recurrent costs for public administrations (personnel and maintenance)					73.170.067,09	1	1	1	73.170.068		100%		
5										0,00			0	0		100%		
6										0,00			0	0				
7										0,00			0	0				
8										0,00			0	0				
9										0,00			0	0				

Proposal On A Common Approach to the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes If the act assessed is the transposition of an act adopted at another level, insert here the name and reference of that 'original' act						Tariff (€ per hour)		Time (hour)		Price (per action or equip)	Freq (per year)	Nbr of entities	Total nbr of actions	Total cost	Regulatory origin (%)			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group	i	e	i	e						Int	EU	Nat	Reg
												Total administrative cost (€)		206.151.529				

explanation: type of obligation "other": refers to the receipt of the PNR information by the passenger information units, screening of data and transmission to law enforcement authorities (TBC).

Airlines Statistics from Eurocontrol show a total number of XXX European carriers operating international flights in 2006. XXX of these carriers operate less than 1000 flights per year. **non-recurring cost** source Lufthansa (costs incurred in joint project with 5 other European airlines.		
Cost for European airline of PULL system to USA:	€ 200 000,00	
Cost for European airline of PUSH system to USA/Canada:	€ 600 000,00	
Additional costs would have to be borne for increasing the capacity of existing systems to cope with EU PNR obligations. It is assumed that this would double the costs mentioned above.		
Total estimated cost for European airline for setting up PULL:	€ 400 000,00	
Total estimated cost for European airline for setting up PUSH:	€ 1 200 000,00	
Total number of outbound flights operated by EU carriers per year (2006, source Eurocontrol)		560 236
Within which total number of LH-operated flights		57 721 **(10,3%)**
Extrapolation of set-up cost of PUSH to total number of flights operated by EU carriers	**€ 11 647 116,00**	
Assuming an amortisation period of 5 years, the yearly cost would amount to:	**€ 2 329 423,00**	.
Carriers with less than 1000 international outbound flights per year (representing 13% of the total number of flights) are expected to use the intermediary method of transmission, which would diminish		

non-recurrent costs. This administrative costs calculation is limited to costs for EU carriers, which account for 49% of international flights. Estimating the costs of non-EU carriers was not judged feasible due to the diverse economic conditions applying there. source Lufthansa (costs incurred in joint project with 5 other European airlines. **recurring cost** extraction/transmission ***1) push/pull*** CA push US pull source: Lufthansa		
Estimated cost of one push per PNR (source: data from EU flights to CA) in EUR:	€ 0,04	
Estimated cost of one pull per PNR (source: data from EU flights to US) in EUR:	0,03	

total number of passengers flying in and out of Europe per year (source eurocontrol)		56 000 000
EU carriers operate 49% of international flights and will be obliged to use the PUSH system.		
It is assumed that out of the 51% of non-EU carriers, 50% would resort to PUSH and 50% PULL. For the purpose of this calculation, only the cost for EU carriers is calculated.		
Number of passengers on EU carriers on international flights:		27 440 000
Yearly transmission cost for EU carriers using PUSH:	**€ 1 125 040,00**	
Yearly cost for EU carriers using PUSH twice per passenger:	**€ 2 250 080,00**	
2) preparation of PNR personnel and maintenance source: Lufthansa for current US/Canada PNR transmission		
Cost for European airline for personnel	€ 200 000,00	
Cost for European airline for maintenance	€ 80 000,00	
Additional costs would have to be borne for increasing the capacity of existing systems to cope with EU PNR obligations. It is assumed that this would double the costs mentioned above		

Total estimated cost for European airline for personnel	€ 400 000,00	
Total estimated cost for European airline for maintenance	€ 160 000,00	
Share of Lufthansa in total number of outbound flights operated by EU carriers per year		**10,3%**
Extrapolation of personnel and maintenance costs of EU carriers based on the above	**€ 5 435 321,00**	
Carriers with less than 1000 international outbound flights per year (representing 13% of the total number of flights) are expected to use the intermediary method of transmission, which would substantially diminish personnel and maintenance costs. This administrative costs calculation is limited to costs for EU carriers, which account for 49% of international flights. Estimating the costs of non-EU carriers was not judged feasible due to the diverse economic conditions applying there. **Public administrations** **non-recurring costs** source UK		
estimation of setting up costs for a big MS (soft and hardware) for API and PNR	€ 250 000 000,00	
It can be assumed that the proportion of costs for PNR are substantially lower than for API, as API covers all modes of transport in that MS. Therefore, it is assumed that 30% of set-up costs are for PNR.		
Estimated hard- and software costs for a big MS for PNR:	€ 75 000 000,00	
It is assumed that international flights of EU carriers from the UK are predominantly operated by UK companies:		
Number of outbound flights operated by UK companies: source Eurocontrol)	€ 68 340,00	
Share of these flights in the total number of outbound flights (EU carriers):		12,2%
Extrapolation of hard- and software costs for MS based on the above:	**€ 614 833 187,00**	
Assuming an amortisation period of 5 years, the yearly cost would amount to:	€ 122 966 637,00	
Member States with few international flights are expected to use the option of having common		

Units with one or more Member States in which case the non-recurring costs are expected to substantially less **<u>recurring costs</u>** **personnel** Source UK		
Estimated number of FTEs for running a central passenger information unit dealing with API and PNR in a big MS:		100
It can be assumed that 70% of this personnel is working on API.		
Estimated number of FTEs working on PNR in a big MS:		30
Share of UK in the total number of outbound flights (EU carriers):		12,2%
Total number of FTE required for operating PNR in all MS:		246
estimated hourly wage in EUR (average emplyoyment costs + 50% overheads)		27
(EU 25 figures by Mercer Consulting, 11 April 2005, www.mercerhr.com/pressrelease/details.jhtml/dynamic/idcontent/1175865)		
working hours per year (8 hours * 20 days * 11 months)		47 520
total yearly personnel costs for all MS	**€ 11 686 749,00**	
maintenance		
In analogy to the maintenance costs for airlines, this is calculated as a percentage of set-up costs maintenance costs for airlines are 10% of set-up costs. The same ratio is assumed for public administrations.		
total yearly maintenance costs for all MS:	**€ 61 483 319,00**	
sum total yearly maintenance and personnel costs for all MS:	€ 7 3170 068,00	