EUROPEAN COMMISSION

Brussels, 2.2.2011
SEC(2011) 132 final

COMMISSION STAFF WORKING PAPER

IMPACT ASSESSMENT

Accompanying document to the

Proposal for a

EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE

on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

{COM(2011) 32 final}
{SEC(2011) 133 final}

Impact Assessment

on a common approach to the use of Passenger Name Record data

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Organisation and timing

Passenger Name Record (PNR) data are unverified information provided by the passengers and collected by carriers for their own commercial purposes.

A European policy in this area was announced in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" in December 2003[1]. 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"*. Moreover, the Hague programme for 2005-2010 called for a common EU approach to the use of passengers' data for law enforcement purposes.

In this context, on 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes[2] ('the 2007 proposal'). The proposal was accompanied by an Impact Assessment[3] ('the 2007 Impact Assessment') on which the Commission's Impact Assessment Board delivered a positive opinion on 5 September 2007[4]. The proposal was extensively discussed in the Council working groups and the progress made in the discussions was endorsed by the JHA Councils in January, July and November of 2008. The discussions on the proposal in the working groups allowed consensus to be reached on most of the provisions of the proposal[5].

Upon the entry into force of the Treaty of Lisbon on 1 December 2009, the Commission proposal not yet adopted by the Council[6] became obsolete. This was due to the change of the legal basis of the proposal and a change of the decision-making procedure from the consultation procedure to the co-decision procedure. 'The Stockholm Programme – An open and secure Europe serving and protecting the citizens'[7] calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

---

1 COM (2003) 826 final
2 COM(2007) 654
3 SEC (2007) 1453
4 SEC(2007) 1457
5 Council Document 5618/2/09 REV 2 of 29.6.2009
6 The European Parliament adopted a resolution on the proposal on 20.11.2008 - P6_TA (2008)0561
7 Council document of 2/12/2009 17024/09

1.2. Consultation and expertise

For the purposes of the Impact Assessment accompanying the 2007 proposal, the Commission departments consulted all the relevant stakeholders on the basis of a questionnaire which was sent out in December 2006. Subsequently, the Commission invited the Member States to a meeting in Brussels on the 2nd of 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 (ATA), the International Air Carrier Association (IACA), the European Regions Airline Association (ERA) and the International Air Transport Association (IATA). The replies were summarised in the 2007 Impact Assessment which accompanied the 2007 proposal.

Extensive discussions have also been held since 2003 with carriers, data protection authorities and border and law enforcement authorities during the negotiations for the agreements on the transfer of PNR data to the United States, Canada and Australia. The Article 29 Working Party issued a number of opinions on the use of PNR data in relation to international agreements[8]. The implementation of the 2004 PNR agreement with the United States[9] was subject of a joint review by the Commission, assisted by national authorities, and United States. authorities in September 2005. The implementation of the 2007 PNR agreement with the United States[10] was also reviewed by the Commission, assisted by national authorities, and United States. authorities in February 2010. The PNR agreement with Canada[11] was also jointly reviewed in November 2008.

Following the adoption of the Commission's 2007 proposal, all the relevant stakeholders published their positions on it.

The position of the Member States is reflected in the latest version of the proposal which was discussed in the Council working groups in June 2009[12]. The Member States in general agreed with the policy lines suggested by the Commission. In their contribution they suggested the exclusive use of the "push" method, the shortening of the data retention period, the clarification of the uses of PNR data and the adoption of a specific data protection framework for the proposal. A few Member States favoured extending the purpose so as to also cover irregular migration and border controls, while other Member States favoured an extension of the

---

8 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 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.

9 OJ L 183/83, 20.5.2004 and OJ L 235/11, 6.7.2004

10 OJ L 204/16, 4.8.2007

11 OJ L 91, 29.3.2006 p.53, OJ L 91, 29.3.2006 p.49 and OJ L 82, 21.3.2006 p.15

12 Council Document 5618/2/09 REV 2 of 29.6.2009

geographical scope of the proposal in order to include intra-EU flights arguing that the necessity of processing PNR data did not change depending on whether a flight is internal or external.

The main criticism expressed in the Resolution of the European Parliament was that the 'necessity' of the proposed actions had not been sufficiently demonstrated. It questioned whether the proposal met the standard for justifying an interference with the right to data protection. The Resolution expressed the Parliament's concern that the added value of the proposal in the light of other border initiatives had not been assessed. In terms of data protection the European Parliament called for a clear purpose limitation and a better justification of the retention period and stressed that sensitive data should be used only under certain conditions and that data should be transmitted using exclusively the "push" method. It further called for restrictions of onward transfers to third countries, while stressing that only specific authorities should have access to PNR data. Finally the European Parliament expressed concerns that the proposed method of automatically assessing PNR data on the basis of fact-based assessment criteria was a very wide use of the data and recalled that such assessment should never result in "profiling" on the basis of sensitive data.

The Article 29 Data Protection Working Party adopted an opinion on the proposal on 5.12.2007[13]. It considered that the proposal was disproportionate and that it might violate the right to data protection. It called into question the data protection regime as the Framework Decision 2008/977/JHA does not cover domestic processing of data. It considered that the justification for the necessity of the proposal was inadequate, that the data retention period was disproportionate and that only the "push" method of transmission of data should be used.

The European Data Protection Supervisor (EDPS) also issued an opinion on the proposal[14]. This opinion questioned whether the "necessity" and "proportionality" of the proposal had been demonstrated since the proposal concerned a very wide collection of data of innocent people. The EDPS criticised the proposal as leading towards a "surveillance society" and called into question the data protection regime as domestic processing of data is not covered by the Framework Decision 2008/997/JHA. The EDPS specifically suggested to better defining the authorities which would have access to PNR data and the conditions for transferring data to third countries

The Fundamental Rights Agency issued an opinion on the proposal after being requested to do so by the French Presidency of the Council[15]. It was also of the opinion that the "necessity" and "proportionality" of the proposal had not been demonstrated and it considered that there should be more guarantees in the proposal so as to avoid profiling on the basis of sensitive data.

Some airline associations, namely the International Air Transport Association (IATA) and the European Airlines Associations (EAA) issued opinions on the proposal. These associations mainly criticised the decentralised structure of the proposal and stressed that a centralised collection of the data would have financial advantages to the carriers. They also criticised the

---

13 Opinion number 145 of 5.12.2007

14 OJ C 110, 1.5.2008

15 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf

choice of the "push" method and called for the choice of transmission method to be left to the carriers.

Even though the 2007 Impact Assessment received a positive opinion from the Impact Assessment Board and the Commission considered that a legislative proposal was necessary, it was deemed preferable to nevertheless carry out a new Impact Assessment. The present Impact Assessment therefore aims to answer criticism raised by the above mentioned stakeholders. It also aims to include all the new facts and experience gained since 2007 and to analyse the issues in an updated way The Impact Assessment and any subsequent legislative proposal should reflect the latest positions resulting from the discussions in the Council working parties, the resolution of the European Parliament, the opinions of other relevant bodies, and new information gathered since 2007.

The purpose of this report is to examine the possibility of adopting a new proposal to replace the 2007 proposal on the basis of the TFEU. It aims to assess whether there is a need for a proposal at European Union level to set up a coherent legal framework on the obligation of carriers to transmit PNR data to the relevant competent authorities for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime, whilst ensuring a high level of protection of personal data throughout the Union.

An inter-service group was setup to steer the Impact Assessment work. The steering group consisted of officials from DG HOME, DG JUST, DG RELEX, DG MOVE, SJ and SG. It met on 4.8.2010 and 18.8.2010 to discuss the issues arising from the Impact Assessment and further comments were provided in writing.

1.3. Impact Assessment Board

On 10 September 2010, the Commission's Impact Assessment Board delivered an opinion on a preliminary version of this Impact Assessment report. In the opinion, the Board stated that the Impact Assessment report provides a sound basis for action. It recommended that the report should provide additional information on the following issues:

– Further illustrate, through examples, that PNR data are an effective tool for combating terrorism and serious crime;

– Further clarify the rationale for the geographical scope of the initiative;

– Further discuss the different ranges of data retention periods, the optimal duration of the transition period from 'pull' to 'push', presentation of the position of the Member States and the possibility of voluntary cooperation between Member States as a means of achieving the objectives of the initiative; and

– Further clarify the costs for carriers, public authorities and passengers.

The present version of the Impact Assessment report has been redrafted to take account of those recommendations. Additional information and modifications have thus been introduced to this end in many of its sections.

2. PROBLEM DEFINITION

2.1. Description of the problem

2.1.1. Threat of terrorism and serious crime

Over the last decade the European Union and other parts of the world have experienced a further spread of cross-border crime. Trafficking in human beings and drugs constitute a very serious threat to European society and influence the societal and economic structure of every day life. These crimes are showing a steady increase in the EU[16]. Drug trafficking has risen by between 3% and 24% per year in the EU over the last 8 years, while violent crime has risen annually between 2% and8% in the same period. Facilitation of irregular immigration, smuggling of currency and illegal goods are also serious problems with cross-border elements. According to the EU Source book, there were 143.948 criminal offences per 100.000 population in the EU Member States in 2007 (excluding Italy and Portugal for which data were not made available), ranging from 14.465 offences in Sweden to 958 in Cyprus.

Serious crime and terrorist offences cause severe harm to victims, inflict economic damage on a large scale and undermine the sense of security without which persons cannot exercise their freedom and individual rights effectively.

A study published in 2009[17] for the International Labour Organisation estimated that the cost of coercion from underpayment of wages resulting from trafficking in human beings in 2007 in industrialised economies was $2.508.368.218, while the total for the world were $19.598.020.343.

The 2010 Annual report on the state of the drugs problem in Europe of the European Monitoring Centre for Drugs and Drug Addiction acknowledges the global nature of the drugs problem and the growing and severe drug-related problems. By undermining social development and feeding corruption and organised crime they represent a real threat for the European Union. In Europe we have annual seizures of about 1 000 tonnes of the cannabis and about 1 000 cocaine-related deaths annually. The number of problem opioid users in Europe is cautiously estimated at 1.35 million. As regards the economic and social impacts of drugs, in 2008, 22 EU Member States reported a total labelled expenditure on the drugs problem of EUR 4.2 billion.

Another study of the UK Home Office "The economic and social costs of crime against individuals and households 2003/04" measured the costs incurred in anticipation of crime, such as defensive expenditure, the costs as a consequence of crime, like the physical and emotional impact on the victim and the value of any property stolen and the costs incurred in response to crime, including the costs to the criminal justice system. These costs were measured at £36.166.000.000 in 2003.

---

16 Eurostat 36/2009

17 Measuring the costs of coercion to workers in forced labour-Alexandra Vinogradova, Michaelle De Cock, Patrick Belser

In the meantime, four out of five Europeans wish to see stronger action at EU level against organised crime and terrorism[18].

Europol's EU Organised Crime Threat Assessment 2009 (OCTA 2009) found that most of organised crime threats have an international dimension, with criminal groups trying to traffic and smuggle people, drugs and other illicit goods into the EU. The OCTA 2009 established that, in the majority of cases, the most serious organised crime threats involve international travel. Trafficking in human beings and facilitation of irregular immigration involves third country nationals being trafficked into the EU. In addition, most drugs trafficking also involve international travel, with large quantities of drugs being smuggled into the EU every day. 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 communicate long-distance. It is therefore becoming increasingly important to obtain as much information as possible about the travel of such persons. Because of the transnational and organised nature of these serious crimes, it is important to ensure close cooperation of law enforcement authorities within the EU.

Terrorism currently constitutes one of the greatest threats to security, peace, stability, democracy and fundamental rights. The threat of terrorism is not restricted to specific geographical zones. Terrorists and terrorist organisations can be found both inside and outside the borders of the EU and have shown their capability to carry out attacks and acts of violence against any country. Europol's "EU Terrorism Situation and Trend Report 2010", despite finding that terrorism has decreased in the EU during 2009, stressed that the threat remains real and serious. Most terrorist campaigns have a transnational character with either the involvement of either transnational contacts or travel to attend training camps outside the EU.

The terrorist attacks in the United States in 2001, the aborted terrorist attack in August 2006 aimed at blowing up a number of aircraft on their way from the United Kingdom to the United States, and the attempted terrorist attack on board a flight from Amsterdam to Detroit in December 2009 showed the ability of terrorists to mount attacks, targeting international flights, in any country.

2.1.2. PNR data and their uses

There are some types of data traditionally collected specifically for law enforcement purposes, such as fingerprints and DNA. In executing its mandate to enhance police cooperation, the EU acts in order to streamline the sharing between Member States of such data and other information that might be necessary for criminal investigations or criminal intelligence operations[19]. There are other types of data that are initially collected by Member States for non-law enforcement purposes, for example, data on immigration, asylum, vehicle registration and citizenship, but to which law enforcement authorities are given access for the performance of their tasks. A third category is privately-held or privately-collected (as opposed to the aforementioned publicly-held) data. Access by law enforcement to such data is regulated differently in Member States

[18] Standard Eurobarometer 71.

[19] Council Framework Decision 2006/960/JHA

depending on the type of data and their function. Passenger information such as PNR data are one type of such privately-collected and privately-held data.

PNR data is unverified information provided by passengers, and collected by and held in the carriers' reservation and departure control systems. It contains several different types of information, such as travel dates, travel itinerary, ticket information, contact details, travel agent at which the flight was booked, means of payment used, seat number and baggage information. The PNR data of a certain passenger usually do not contain all potential PNR elements[20], but only those actually provided by the passenger at the time of reservation and information given upon check-in and boarding. PNR data are traditionally collected by air carriers. It should be noted that most non-air carriers usually do not collect such data.

PNR data are different from and should not be confused with Advance Passenger Information (API) data. API data are biographical information taken from the machine-readable part of a passport and contain the name, place of birth, nationality of a person, passport number and expiry date. API data are mainly used for carrying out border checks in advance of a person's arrival or departure. Although in some cases the data are also used by law enforcement authorities in order to identify suspects and persons sought, they are mainly used as a border management tool. API data are used systematically in more than 30 countries around the world[21].

In the EU, the use of API data is regulated by the API Directive[22]. The Directive provides that API data should be made available to border control authorities, at the request of each Member State, for flights entering the territory of the EU for the purpose of improving border controls and combating irregular immigration. Even though their use for law enforcement purposes is permitted by the Directive, this is possible only in limited circumstances.

PNR data are mainly used as a criminal intelligence tool, in particular for assessment, rather than as an identity verification tool. The uses of PNR are unique and are mainly the following:

(i) PNR data make it possible to carry out a pre-arrival and pre-departure assessment of all passengers on the basis of fact-based assessment criteria[23] in advance of the arrival or departure of passengers; this allows authorities to focus on those passengers who fit into the fact-based assessment criteria but who were previously unsuspected, rather than subjecting all passengers to an extensive assessment by border guards,

(ii) PNR data can be made available well in advance of a flight's arrival or departure, and hence provide authorities with more time for processing, analysing and potentially taking action,

---

20 The list of all possible PNR elements has been adopted by ICAO in its Guidelines for the use of PNR data of 2005

21 Some examples include Australia, Brazil, Canada China, Cuba, India, Japan, Mexico, Unites States and several other countries- information sourced from IATA

22 Directive 2004/82/EC of 29.8.2004

23 "fact-based risk indicators" are rules established by law enforcement authorities through the analysis of past PNR data and other relevant intelligence. They are usually the result of trend analysis and aim to set out rules for carrying out the automated risk assessment of passengers. They could relate to ways of travel behaviour, travel routes etc.

(iii) it is possible to match PNR data against databases with specific addresses, telephone numbers, credit cards connected to criminal offences and establish to whom such data belong, and

(iv) by matching PNR data of persons known to law enforcement authorities against the PNR data of persons unknown to such authorities, it is possible to identify associates of suspects assisting in the preparation and execution of a crime.

For several years this is how PNR data have been used, mainly by customs and law enforcement authorities around the world. However, , it was until recently not technically possible for the authorities of a country to access such data electronically and in advance of the flight, so they were only processed manually and only in relation to a limited number of flights. Technological advances have since made the advance electronic transfer, analysis (and subsequent retention) of such data possible.

To address the threat of serious crime and terrorism, law enforcement authorities may use PNR data in several ways:

- **re-actively:** use of the data in investigations, prosecutions, unravelling of networks after a crime has been committed. In order to allow law enforcement authorities to go back sufficiently in time, a commensurate period of retention by law enforcement authorities is necessary.

- **in real time:** use of the data prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR data are especially useful for running such data against predetermined assessment criteria in order to identify persons that were previously "unknown" to law enforcement authorities and for running the data against various databases of persons and objects sought.

- **pro-actively:** use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers. In order to carry out such an analysis of relevance for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, a commensurate period of retention of the data by law enforcement authorities is necessary in such cases.

It is necessary to impose those legal obligations on air carriers for the following reasons:

First, PNR data enable law enforcement authorities to identify persons, who were previously "unknown", i.e. persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved in such crime and who should therefore be subject to further examination by the competent authorities. Identifying such persons helps law enforcement authorities prevent and detect serious crimes including acts of terrorism. To achieve this, law enforcement authorities need to use PNR data both in real-time to run PNR against predetermined assessment criteria which indicate which previously ‘unknown’ persons require further examination and pro-actively for analysis and creation of assessment criteria.

For example, an analysis of PNR data may give indications on the most usual travel routes for trafficking people or drugs which can be made part of assessment criteria. By checking PNR data in real-time against such criteria, crimes may be prevented or detected. A concrete example given by a Member State on trafficking in human beings is a case where PNR analysis uncovered a group of human traffickers always travelling on the same route. Using fake documents to check in for an intra-EU flight, they would use authentic papers to simultaneously check in for another flight bound for a third country. Once in the airport lounge, they would board the intra-EU flight. Without PNR it would have been impossible to unravel this human trafficking network.

The combined pro-active and real-time use of PNR data thus enable law enforcement authorities to address the threat of serious crime and terrorism from a different perspective than through the processing of other categories of personal data: as explained further below, the processing of personal data available to law enforcement authorities through existing and planned EU-level measures such as the Directive on Advance Passenger Information,[24] the Schengen Information System (SIS) and the second-generation Schengen Information System (SIS II) do not enable law enforcement authorities to identify 'unknown' suspects in the way that the analysis of PNR data does.

Second, PNR data help law enforcement authorities prevent, detect, investigate and prosecute serious crimes, including acts of terrorism, after a crime has been committed. To achieve this, law enforcement authorities need to use PNR data in *real-time* to run the PNR data against various databases of 'known' persons and objects sought. They also need to use PNR data in a *re-active* manner to construct evidence and, where relevant, to find associates of criminals and unravel criminal networks.

For example, the credit card information which is part of the PNR data may enable law enforcement authorities to identify and prove links between a person and a known criminal or criminal organisation. An example given by a Member State relates to a large scale human and drug trafficking involving a Member State and third countries. Cartels were importing drugs to several destinations in Europe. They were using drugs swallowers who were themselves trafficked persons. They were identified on the basis of having bought the ticket with stolen credit cards on the basis of PNR. This lead to arrests in the Member State. On this basis, an assessment criterion was created which itself led to several arrests in other Member States and third countries.

Finally, the use of PNR data prior to arrival allows law enforcement authorities to conduct an assessment and perform a closer screening only of persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security. This facilitates the travel of all other passengers and reduces the risk of passengers being subjected to screening on the basis of unlawful criteria such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards.

---

[24] Directive 2004/82/EC of 29 August 2004.

The value of using PNR data in this context is confirmed by information from third countries and Member States that already use PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The experience of those countries shows that the use of PNR data has led to critical progress in the fight against crime, in particular, drugs and human trafficking and the fight against terrorism, and a better understanding of terrorist and other criminal groups through the gathering of intelligence on their travel patterns. 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, build intelligence about terrorists and criminals and identify behaviour patterns of such persons. Even though PNR data are passenger data linked to travel, they are mainly used as a criminal intelligence tool rather than as border control tool. They are used in advance of a border crossing and not at the border crossing itself. Their main aim is to fight terrorism and serious crime rather than fight irregular immigration and facilitate border controls. The Commission adopted on 20.7.2010 a Communication on the Overview of information management in the area of freedom, security and justice[25] the purpose of which was to provide a full overview of EU-level measures in place, under implementation or consideration regulating the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management. This Communication noted that the Schengen Information System (SIS)[26] the second-generation Schengen Information System (SIS II)[27], the Visa Information System (VIS)[28], and the anticipated Entry/Exit System and Registered Travellers Programme[29] are EU measures that deal directly with actions taking place physically at the borders.

The proposal will neither change nor interfere with current EU rules on the way border controls are carried out or with the EU rules regulating entry and exit from the territory of the Union. The proposal will rather co-exist with and leave those rules intact.

PNR data are also useful for other policy purposes. For example, they are useful for immigration purposes to find persons who have exceeded their permitted stay on a visa by providing a record of when a person enters the EU. In aviation security, PNR data could be used to prevent persons who might pose a threat to the security of the aircraft from boarding, through the implementation/establishment of 'no-fly lists'. In relation to health safety, if a passenger is found to be suffering from a highly contagious disease, PNR data could be used to quickly inform passengers on the same flight, in particular those who sat in the immediate surroundings of that passenger

---

25 COM (2010)385, 20.7.2010

26 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, p. 19.

27 Regulation (EC) No 1987/2006, Decision 2007/533/JHA, Regulation (EC) No 1986/2006.

28 Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA. See also Declaration on combating terrorism, European Council, 25.3.2004.

29 […].

2.1.3. Divergence between national PNR systems

Even though only a limited number of Member States have set up a PNR system to date, most Member States use PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime in a non-systematic way or under general powers granted to the police or other authorities. Within the EU, the United Kingdom already has a PNR system, while France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation and/or are currently testing using PNR data. Several other Member States are considering setting up PNR systems, but they are waiting for a proposal from the Commission which will enable them to obtain the full benefits of using PNR.

An analysis of the national legislation of the United Kingdom, France and Denmark[30] indicates that their provisions diverge and can be summarised as follows:

- The United Kingdom provides for the use of PNR data in the fight against terrorism, all crimes and irregular immigration. PNR data will be required from all flights, including intra-EU and domestic flights. The retention period would be 5 years in an active database and 5 years in archives. PNR data will be required from air, sea and rail carriers to the extent that such data exists.

- French legislation provides for the use of PNR data in the fight against terrorism and irregular immigration but not for other crimes. PNR data will be required from all flights, including intra-EU and even domestic flights. The retention period is 24 hours for immigration purposes and 5 years for terrorism purposes in an active database. PNR data will be required from air, sea and rail carriers to the extent that it exists.

- Danish Legislation provides for the use of PNR data only in the fight against terrorism and crimes against the State. The proposed retention period is 1 year and covers only air travel. It does not propose 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 are divergences with regards to 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 likely that once the complete regulatory framework for the use of PNR data in these Member States is adopted, they will diverge, for instance, on data protection rules, the use of sensitive data, rights of access and judicial redress, the role of supervisory authorities and the range of authorities having access to the data. It is also expected that there will be divergences on the measures taken to safeguard the security of the transmission of the data, i.e. different transmission protocols and message formats.

---

[30] For the United Kingdom, 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

As more Member States are preparing their own PNR legislation, this might lead to the creation of up to 27 considerably diverging systems. This could result in uneven levels of data protection across the Union, security gaps, increased costs and legal uncertainty for carriers. This could lead to distortions in the internal market.

2.1.4. Agreements with third countries

The first country that recognised and made use of PNR data in a systematic electronic way was the United States, which, after the terrorist attacks of 9/11, proceeded immediately with the introduction of PNR data legislation. Since then, more countries have followed and passed similar legislation, namely Australia, Canada and New Zealand and more recently Japan and South Korea. Various other countries are also currently working towards such legislation. The EU has signed agreements for the transfer of PNR data with the United States[31], Canada[32] and Australia[33]. These Agreements regulate the transfer of PNR data by carriers operating flights between the EU and these countries for the purpose of the fight against terrorism and transnational serious crime. They also list a series of safeguards that the third country must respect when handling personal data of passengers whose PNR data are transmitted under the Agreements. The Agreements do not deal with transfers of PNR data for flights by carriers to the EU or the authorities of Member States' as the EU does not yet have a PNR system in place. The Agreements only provide, in terms of reciprocity, that the authorities of the third countries share some analytical information with the Member States' authorities. If the EU had a PNR system, the reciprocity element of such Agreements would be implemented more thoroughly.

The Commitments on which the PNR Agreement with Canada was based have expired in 2009 and therefore the Agreement needs to be renegotiated. The Agreements with the United States and Australia are only provisional and have not yet been officially concluded by the EU. Upon the entry into force of the Treaty of Lisbon, the European Parliament proposed that both these Agreements should be renegotiated as they do not provide for adequate protection of personal data. Therefore, the Commission requested that the Council provides it with negotiating directives to enter into new agreements with the United States[34] and Australia[35]. The Commission also recommended that the Council provide it with negotiating directives to enter into a new agreement with Canada[36] as well. The Council adopted the relevant Decisions on 2 December 2010. Other countries, notably Japan and South Korea have also requested to negotiate such agreements.

Through the experience gained by the countries that already use PNR data, the Member States have come to appreciate the full value of PNR data in the fight against terrorism and other serious crime.

---

31 OJ L 204/16, 4.8.2007

32 OJ L 91, 29.3.2006 p.53, OJ L 91, 29.3.2006 p.49 and OJ L 82, 21.3.2006 p.15

33 OJ L 213, 8.8.2008, p.49

34 SEC(2010)1082, 21.9.2010

35 SEC(2010)1083, 21.9.2010

36 SEC(2010)1084, 21.9.2010

2.1.5. Types of carriers collecting PNR data

Currently only air carriers collect PNR data. Sea and rail carriers do not collect such data, with some exceptions. For example, some rail and sea carriers collect PNR-like data for instance the Eurostar. and Thalys collect some data when the reservation is made online and cruise ships collect some PNR-like data as well. On the other hand, ferries and trains other than the Thalys and the Eurostar do not have computerised reservation systems which are similar to those of air carriers.

The collection of PNR data by carriers should also be considered against the background of increasing passenger flows. According to the data provided by the Member States, there were 767 million external border crossings in 2007 and 714 million in 2008. It should be noted that the data are not fully comparable because the Schengen enlargement in 2007 (land borders) and 2008 (air borders)[37] shifted the physical location of the Schengen external border and affected the number of external border-crossing points. Furthermore, Member States do not record such movements in a consistent manner, so rates are based mainly on estimations. However, based on discussion with Member States it can be assumed that border-crossings at the largest and busiest points have been increasing and will continue doing so in the future[38].

In addition, the total number of travellers differs a lot between Member States with some Member States recording over three million travellers crossing the borders in a one week period and others recording below 50.000 travellers.

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[39]. With an annual rate of increase of these flights of 7.7%[40], the number of flights going in and out of the EU-27 in 2010 was 4.500.000.

2.2. EU right to act and subsidiarity principle

The right of the EU to act in this field is enshrined in Articles 82 and 87 of Title V of Chapter V of the Treaty on the Functioning of the European Union (TFEU).

As the threat from terrorism and cross-border serious crime remains significant, it is important to provide law enforcement authorities with new effective tools with which to perform their tasks. As most of the categories of serious crimes, like drugs and human trafficking, often involve international travel, it is essential that authorities collect, process and exchange PNR data to increase the internal security of the EU. Moreover investigations for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes carried out by the

---

37 The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia joined the Schengen area in 2007 (air borders were lifted in 2008).

38 See also the World Trade Organisation (WTO) forecast: Tourism 2020 vision, http://www.wto.org/english/tratop_e(ser_e/omt.ppt and the travel forecast of Office of Travel and Tourism Industries (OTTI), http://tinet.ita.doc.gov/view/f-2000-99-001/index.html.

39 Figures according to Eurocontrol on the basis of CFMU IFR Flights

40 Eurocontrol Annual Report 2009

competent authorities of the Member States are largely dependent on international cross-border cooperation.

Because of the free movement of persons in the Schengen area, it is necessary for all Member States to collect, process and exchange PNR data, in order to avoid security gaps due to criminals diverting their planned journeys through Member States not collecting PNR data. By acting collectively and coherently this measure will have a substantial impact on the security of the EU.

If Member States are left to legislate independently on issues such as data retention periods, use of sensitive data, purpose limitation, push/pull methods and onwards transfers to third countries, safeguards might diverge. Action at EU level will help to ensure harmonised provision on safeguarding data protection throughout the Union.

A further reason why EU action would be more appropriate is that differences between national requirements adopted in Member States that have already established similar mechanisms or which will do so in the future, may impact negatively on the air carriers as they may have to comply with several potentially diverging requirements. Different standards regarding the method of transfer of data, the messaging format, the data security mechanisms, the frequency of transmissions etc, would be very costly for carriers operating in different Member States to implement.

On the basis of the above, it can be concluded that the EU is both entitled to act and better placed to do so than the Member States acting independently. Such an action should not go beyond what is necessary to achieve its objectives.

2.3. How would the problem evolve, all things being equal?

Without action at EU level, it is likely that several Member States will implement their own domestic PNR systems. This would mean that the full benefits offered to develop the fight against terrorism and serious crime to increase internal security of the Union, by cooperating on PNR data collection, would not be attained. This would also mean that the Union might end up with various diverging PNR systems leading to negative effects on the internal security of the Union, by the potential creation of serious security gaps.

The development of different and diverging PNR systems in the Union could also have an adverse effect on the level of protection of personal data afforded to passengers, since the standard of data protection in the Member States may vary, despite respecting the general European standards. As more and more Member States adopt national legislation for the use of PNR data and as more and more third countries request such transmission from carriers, it is important to ensure uniform and high level protection of personal data when processing PNR data. Sufficient safeguards should be provided to ensure that passengers have access to enforce their rights. The Article 29 Data Protection Working Party, despite opposing the use of PNR data, strongly prefers a European instrument with robust data protection guarantees to various national systems with diverging data protection standards.

In addition, diverging PNR systems in the Union would create difficulties for carriers 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 this reason, the carrier associations which were consulted for the purposes of this report were strongly in favour of harmonising the use of PNR data at EU level.

Another aspect to be taken into account is that the number of travellers continues to increase. This, together with additional border and security controls, has started creating problems of managing the flows of passengers efficiently. This problem is expected to worsen as the number of passengers increase. 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 passenger's PNR data before he or she actually arrives in the country of destination will make it possible to clear non-identified travellers and subject them only to minimum controls at the border.

3. POLICY OBJECTIVES

3.1. Objectives

One of the fundamental goals of the Union is the development of a genuine European area of justice, freedom and security. Such an area aims to ensure that the fundamental rights of individuals living in the EU, such as the right to life, physical integrity and the protection of personal data and privacy, are guaranteed.

The general objective is therefore to increase the internal security of the EU, while respecting the right to protection of personal data and other fundamental rights. This is in line with the Stockholm Programme, which calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and other serious crime.

This general objective translates into the following specific policy objectives:

(1) To prevent and reduce terrorist activities and other serious crime through a global approach to the use of PNR data avoiding security gaps. At operational level, the objective would be to collect and process PNR data in an electronic format in order to benefit fully from the advantages offered by modern technologies for such use.

(2) To ensure that individuals' right to the protection of personal data is duly respected when PNR data are collected and processed. At operational level, the objectives is to facilitate the exchange of PNR data among responsible authorities and to ensure that access to PNR data is limited to what is necessary for the pre-defined purpose(s).

(3) To provide legal certainty to and reduce costs for carriers. There are two operational objectives, to reduce differences in legal and technical requirements imposed on carriers and to avoid distortion of the internal market due to diverging legal requirements.

3.2. Respect of fundamental rights

The impacts on fundamental rights in the Impact Assessment have been assessed in line with the Fundamental Rights "Check List" as provided for in the Commission's Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union[41].

The purpose of any proposed measure would be to prevent and combat terrorism and other serious crime so as to increase the public security in the EU and safeguard fundamental rights.

The use of PNR data would involve the collection, processing, exchange and use of personal data of individuals for public policy purposes. As such, this processing interferes with the fundamental rights to the protection of private life and to the protection of personal data as recognised by Articles 7 and 8 of the Charter on Fundamental Rights of the European Union and Article 8 of the European Convention of Human Rights, as well as Article 16 of the Treaty on the Functioning of the European Union. The right to private life and to the protection of personal data is however subject to limitations and conditions defined in Article 8 of the European Convention of Human Rights and Article 52 of the Charter on Fundamental Rights of the European Union. These limitations permit interferences that are in so far as 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". "in accordance with the law" and "necessary in a democratic society". As the proposed actions would be for the purpose of combating terrorism and other serious crime, contained in a legislative acts they would clearly comply with such requirements provided they are "necessary in a democratic society" and comply with the principle of proportionality.

Any proposed action would fall within the scope of Title V of Chapter V TFEU on police and judicial cooperation. The Data Protection Directive 95/46/EC[42] would not apply as actions within a framework established by public authorities to safeguard public security are excluded. The provisions of the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[43] would apply to data exchanged between Member States but not to the domestic processing of personal data for law enforcement purposes, leaving a protection gap at national level. Since any proposed measure would involve domestic processing of PNR data by Member States, it is necessary to devise data protection rules for such processing. The most suitable solution in the circumstances would be that the data protection safeguards of any proposed measure are in line with the Framework Decision 2008/977/JHA. On this basis, any proposed action should ensure that the purpose of the use of PNR data is clearly defined, that processing of personal data is secure, that the right of individuals to information, access, rectification, erasure and blocking are respected, and that Member States impose liability, appropriate sanctions and remedies. Equally, the supervision of

---

41 COM (2010)573 of 19 October 2010

42 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p 31, Article 3

43 Council Framework decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the Framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p.60.

the application of these rules by the data protection supervisory authorities in Member States, exercising their functions with complete independence, is an essential component for efficient protection of personal data under any such proposal.

This solution would guarantee a uniform standard of protection of personal data under any proposal, and provide legal certainty for individuals, commercial operators and law enforcement authorities.

4. POLICY OPTIONS AND TRANSVERSAL ISSUES

4.1. Policy options

In order to achieve the objectives mentioned above, the Commission considers that there are four main policy options described below:

A. Refraining from addressing the issue at EU level – Maintaining the status quo

This policy option involves no action being taken by the EU. This means that the issue of processing and exchanging PNR data will remain unresolved at EU level while different and largely diverging solutions to the processing and exchanging of PNR data would be developed and implemented by Member States acting independently.

Three Member States have already started implementing national PNR data systems and it is expected that more will follow.

B. Options addressing the structure of a system for collecting and processing PNR data

B.1: Decentralised collection and processing of data by Member States

This policy option would involve an EU legislative instrument to ensure that Member States collect, process, use and share certain categories of PNR data for specific purposes. Each Member State would be required to collect and process the PNR data of travel to and from its territory, while sharing relevant PNR data or analysis of PNR data with other Member States. Therefore each Member State would be individually as well as collectively responsible for increasing the internal security of the EU. Under this option, the Member States would bear the costs of establishing their national PNR systems. Consequently, it would be Member States that decide on how best to use PNR data, within the limits of the EU legislative instrument. These activities would be subject to a number of safeguards aimed to comply with data protection requirements and the security of data transfers. Such safeguards should include appropriate purpose limitation, clearly defined periods of retention, and rules ensuring the security of data processing as well as redress mechanisms.

B.2: Centralised collection and processing of data at EU level

This policy option would involve an EU legislative instrument to require that an EU central unit collects, processes, uses and shares with Member States certain categories of PNR data for defined purposes. It would involve the centralised collection and processing of the data by an EU

body, rather than requiring each Member State to collect and process the PNR data of travel to and from their territory. Carriers would be obliged to transmit the PNR data of their passengers to a Centralised Unit at EU level which would filter out the non-required data when necessary, process and share PNR data or analysis of PNR data with the relevant authorities of the Member States. The Centralised Unit would be responsible for retaining the data. Consequently, the EU would be responsible for processing and retaining the data, within the limits of the legislative instrument. These activities would be subject to a number of safeguards aimed at providing the highest level of protection of personal data and a secure transmission of the data. Such safeguards should aim at ensuring the appropriate purpose limitation, defining the retention period, and setting rules for the security of the data and redress mechanisms. The work of such a unit would be substantial, it would require an important number of staff and it would need to work on a 24/7 basis. Under this option, the EU, together with each Member State would be collectively responsible for increasing the internal security of the EU. The costs for establishing and running the system would be borne by the EU budget.

C. Options addressing the purpose limitation of the proposed measures

C.1: Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime only

Under this option, PNR data would be used for the prevention, detection, investigation and prosecution of terrorist offences and other serious crimes**.** The term "terrorist offence" could be defined according to the Framework Decision on combating terrorism 2002/475/JHA[44]. The term "serious crime" could be defined according to the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedure between Member States. This option would be consistent with the approach of the Commission as regards transfers of PNR data to third countries, as set out in the Communication on the global approach to transfers of PNR data to third countries and with its general approach in police and judicial cooperation instruments.

C.2: Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and other policy objectives

Under this option, PNR data would be used not just for the prevention, detection, investigation and prosecution of terrorist offences and other serious crime, but also for other purposes, such as immigration control, aviation security and health safety, described in section 2.1.2.

D. Options addressing the modes of transport to be covered by the proposed measures

D.1: Air travel only

Under this option, PNR data would be collected only for air travel. Currently only air carriers regularly collect such information. The data are provided by the passenger voluntarily and are collected and processed by the air carriers for commercial purposes via their reservation and

[44] OJ L164, 22/6/2002, p.3

departure control systems. The nature of air travel requires that at least the name and flight number for each passenger are known at the time of booking.

D.2: Air, sea and rail travel

Under this option, PNR data would be collected for air, sea and rail travel. Because most sea and rail carriers do not currently regularly collect PNR data, this option involves extending the collection of PNR data to those types of carriers.

E. Voluntary/enhanced cooperation

This option would result in the issue being dealt with by encouraging cooperation between the Member States. Such cooperation could take the form of exchanges of best practices. However, it is considered that the option of encouraging cooperation between Member States, would not achieve the desired objectives. Firstly, it would be extremely difficult, if not impossible, to ensure a common EU approach, and it would be impossible to ensure that such best practices are actually being exchanged. Moreover, the problems of terrorism and organised crime affect all Member States and are not only limited to some Member States. If Member States refuse or fail to coordinate their activities, they would create a substantial security gap within the Union. The security of the EU is the joint responsibility of Member States and they should all act in a harmonised manner to achieve the desired results. The goal of increasing security can therefore not be sufficiently achieved merely by encouraging cooperation between Member States. In addition, the airlines and the data protection authorities of the Member States generally opposing the idea of using PNR data for law enforcement purposes were adamant that if any action were to be taken it should involve harmonisation. Otherwise it is likely that we will end up with diverging requirements which will ultimately be very costly for the airlines and the Member States. 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 cooperation.

On the basis of the above, the option of encouraging cooperation between the Member States in this field is rejected at this initial stage and will not be further examined.

4.2. Transversal issues

There are a number of transversal issues which arose from the consultations with Member States and other stakeholders that are relevant to the use of PNR data but which are not presented as policy options in the present report, either because there is already a general consensus on these issues or because an alternative approach to the one presented is not considered realistic at this stage. This section provides an overview of a preliminary analysis of these issues.

4.2.1. Geographical scope

It would be most reasonable and proportionate that any proposed measure would apply to travel from a third country to or from a Member State. This would ensure that PNR data of all passengers entering or departing from the EU would be collected, processed and retained.

Member States and the EU would undertake to act individually and as well as collectively to increase security in the EU.

Given that the objectives pursued by the collection of PNR data are the same inside and outside of the EU, there would be an important added value in including internal flights, i.e. flights between Member States in any proposed measure. Making the instrument applicable to all travel, including internal travel, though favoured by some Member States, is however considered premature at this stage. Considering the large number of travellers on internal flights, which is three times more than the number of passengers on international flights[45], the costs for setting up and operating the system would be much higher. The hardware and software required to set up the system would have to have a much larger capacity, and therefore would be much more expensive. A system including internal flights would be too ambitious to adopt as a first step, but it is one that should be considered for the future, as part of a step-by-step approach. The possibility and necessity of including internal flights in any measure could be the subject of an in-depth evaluation a couple of years after the measure has been in operation. The experience of those Member States that collect PNR data on internal flights by that point should be taken into account for the purposes of the evaluation.

4.2.2. Sensitive data

As regards the processing of sensitive data, any proposed measure should be consistent with the 2007 Impact Assessment and the 2007 proposal ensuring that "sensitive" data[46], to the extent that they are contained in the PNR data, are filtered out and deleted immediately.

4.2.3. Data retention period

On the length of the data retention period, a commensurate period of retention of the data by the relevant authorities is necessary when using PNR data re-actively or pro-actively. The option of deleting the data upon the arrival of the passengers at the country of destination does not seem appropriate as it would limit the potential of PNR data to one of the three possible uses listed in 2.1.2, namely real-time use. Such a limitation would not make full use of the added value of using PNR data.

The retention period should not be longer than necessary for the performance of the tasks for which PNR data are used and should take into account the different ways in which PNR data are used and the possibilities of limiting access rights over the period of retention. The 2007 Impact Assessment and 2007 proposal set the active retention period to 5 years and retention in an inactive database for another 8 years. This choice was heavily criticised by the data protection stakeholders and the European Parliament as too long and disproportionate. For the purposes of this report, it is proposed that any new measure should provide for a reduced period of data retention. Such a data retention period should also provide for the gradual reduction of access

---

45 Eurocontrol Annual Report 2009

46 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, i.e. personal data revealing racial origin, political opinions or religious or other beliefs, or concerning health or sexual life

rights, for example through anonymising the data**.** The solution should meet the concerns expressed by Member States and must draw on experience gained from international agreements that the EU signed in the field. It must represent the absolute minimum of what is required for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and what can be considered acceptable from a data protection point of view. The chosen period must meet data protection requirements.

On the basis of the above, and taking into account the data retention periods in the countries that currently use PNR data, the period of retention should be one year with an additional period of five years in an anonymised database.

4.2.4. Push/pull

As regards the method of transmission of the data by the carriers, the "push" and "pull" methods were considered.

With the "push" method carriers transmit (push) the required PNR data into the database of the requesting authority. On the other hand with the "pull" method, the requesting authority can reach in to the carrier's reservation system and extract (pull) a copy of the required data into their database.

The advantages of the "push" method over the "pull" method are undisputable, as public authorities can keep control over what happens with the databases located on their territory. Another advantage would be that the public authorities keep control over the security of the data transfers. The risks of the "pull" method are that the authority which receives the data potentially may access all data in the databases of the carriers and would then have to filter them out themselves. The carriers are therefore left with no control over the data they have collected and for which they are responsible.

It is important to stress that the transmission of PNR data by carriers to public authorities generates a substantial cost for carriers[47], with the "push" method being substantially more costly than "pull" method. Carriers would have to implement "push" method from a hardware and software point of view. They would then have to pay the transmission costs (telecommunication lines) for each "push" of the data. As such, the actual cost for carriers will depend on the carrier's size and the number of flights that it executes under any proposed measures. Therefore, small carriers, with few flights would have fewer costs. The system's hardware and software would need to be of a smaller capacity and the transmission costs would not be substantial. On the other hand, large carriers with many flights will need systems with bigger capacity and many more telecommunication lines.

The risks however to the protection of the data of passengers with the "pull" method clearly outweigh the advantages that it offers in relation to costs.

[47] Detailed explanations and figures on costs are provided in Annex A and Chapter 7 of this Report.

Even though the 2007 Impact Assessment and 2007 proposal had proposed the use of the "push" method for EU carriers and a combination of "push" and "pull" methods for third country carriers, the data protection stakeholders and the European Parliament criticised this decision and insisted on the exclusive use of the "push" method. In response to these criticisms and in further consultations with the Member States, it is advisable that any proposed measure should provide for the exclusive use of the "push" method by all carriers. Even though the "push" systems are currently being developed, it requires a certain timeframe to become fully operational. More specifically, carriers will have to implement the "push" method, adopt the necessary data formats and encryption methods and develop links to all relevant Member States in order to transmit the data. Member States would also have to implement the "push" method on the receiving side, adopt the necessary technical requirements and links with the carriers. All these processes are complex and difficult to implement and air carriers and Member States should do their utmost to comply with this method.

4.2.5. Automated Individual Decisions

One of the biggest criticisms of the use of PNR data for trend analysis and for running it against the fact-based assessment criteria is that it might result in what is critically referred to as 'profiling'. Profiling can be described as an automatic data processing technique that consists of applying a "profile" to an individual, in order to take decisions affecting him or her. EU data protection legislation in principle grants every individual the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based exclusively or to a decisive extent on automated processing of data intended to evaluate certain personal aspects relating to him.[48] A person, however, may be subjected to a decision of this kind if it is authorised by law which also lays down measures to safeguard the data subject's legitimate interests. Any proposal for the use of PNR data should therefore comply with this data protection principle and lay down effective measures to safeguard the data subject's legitimate interests. Such measure could include that any automated individual decisions has to be verified and confirmed by a human being and allow for arrangements allowing the data subject to present his or her point of view.

4.2.6. Scope of the data

As regards the issue of the scope of the data, the competent authorities should be able to use only those elements of PNR data considered proportionate and necessary for the fulfilment of the purpose of the specific measure. Any list of PNR categories to be used should include the minimum of what is necessary and the maximum of what is proportionate to fulfil its purpose in this specific case. It is also important to note that any measure should not oblige carriers to introduce mandatory fields in their collection of PNR data from their passengers. The carriers should continue to collect and make available to the competent authorities only those data voluntarily provided by the passenger for the reservation of the flight or which have been collected following check-in and boarding.

---

[48] Article 15 of Directive 95/46/EC; Article 7 of Framework Decision 2008/977/JHA.

4.2.7. Data to be transmitted from the Passenger Information Units/Centralised Unit to the competent authorities

Data can be transmitted to the competent authorities either in bulk or on a case-by-case basis.

It seems preferable that the carriers do not filter the data which they will transmit to the competent law enforcement authorities. This filtering could best be done by the Passenger Information Units designated by the Member States or by the EU Centralised Unit (depending on which option is finally adopted). The Passenger Information Unit or Centralised Unit would thereby filter out the non-required data and run the PNR data through the alert systems and the assessment criteria in order to identify suspicious passengers. The Unit would then transfer only the PNR data of identified passengers to the relevant authorities. In addition, the relevant authorities could make specific requests to the Unit for the provision of data in relation to specific investigations or to assist in analysing the data. These authorities will not have access to the PNR data of other passengers. In this way, the possibility of abuse of the data would be reduced. 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.

4.2.8. Bodies receiving data from the Passenger Information Units

The Passenger Information Units/Centralised Unit should process and then transfer to the competent national authorities of the country of destination/departure, only the PNR data of the identified passengers. They should also transfer the PNR data of the identified passengers to the Passenger Information Units of the other Member States, which should then, in their turn, transfer them to their national law enforcement or other competent authorities.

5. ANALYSIS OF IMPACTS

This section identifies 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. The most significant impacts will be analysed below against the following criteria: security in the Union, protection of personal data, costs for public authorities, costs for carriers/competition, the internal market and aim to encouraging a global approach. Impacts are rated as absent, small, medium or significant:

Table of symbols (using (-) for negative and (+) for positive impacts)	
Small impact	- / +
Medium impact	-- / ++
Significant impact	- - - / +++
No impact	0

5.1. Impacts of the option of refraining from addressing the issue at EU level – Maintaining the status quo (Policy Option A)

This policy option entails no action to be taken by the Union. The status quo will therefore remain. The status quo, as explained, is that currently three Member States have relevant legislation for the use of PNR data. The consultations however, suggested that in the very near future, more and more Member States will start adopting similar internal measures as well. Therefore, in our assessments, the status quo also takes into account expected developments in the very near future.

Increasing security in the EU (0): A "no action" policy will impede the ability of the EU to fight terrorism and serious crime and hence have a negative effect on the security in the Union. This would mean that the full advantages offered by PNR data to the security of the EU, would not be attained. This would also mean that the Union might end up with various diverging PNR systems, leading to negative effects on the internal security and the creation of security gaps. The Union will have fewer means of identifying terrorists and criminals. Furthermore, it will deprive the Member States of a very important source of obtaining intelligence on terrorists, criminals and their associates. Nevertheless, if some Member States develop their own systems, the impact on increasing the security in the Union will be positive but to a lesser extent than if action is taken collectively. Terrorists and criminals might choose to enter the Union through a Member State which does not have such a system or a system with lower standards. In addition, in view of the free movement of persons within the Schengen area, a system introduced in one Member State might prove to be insufficient, as it cannot go beyond its territory**.** Therefore the aim of substantially increasing the security of the Union cannot be sufficiently achieved merely by relying on national measures.

Increasing the protection of personal data (0): Each Member State which develops a national system would have to safeguard the right to data protection of passengers. The standards of data protection might vary depending on which Member State a passenger travels to or from. For example, data might be retained for different periods in different Member States, some Member States might use sensitive data while others do not, Member States might have different standards for notifying passengers of the processing of their data or provide different levels of access to data. More importantly, Member States might use the data for different purposes, for example some might use the data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and immigration purposes, while others might exclude immigration. Some may use the data for all types of crimes while others limiting the use to serious crimes. Member States might have wide exceptions as regards the access to data or in relation to redress. Such divergence of standards would be undesirable as passengers would have different rights depending which Member State they travel to and from. The data protection authorities would deplore such a development and the Article 29 Working Party on Data Protection and the European Data Protection Supervisor are adamant that in case Member States start implementing national measures, harmonised EU action would become necessary**.**

Costs on public authorities (0): Public authorities in Member States deciding to introduce national PNR legislation would need to set up systems to receive data from carriers. This is likely 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. Each national authority would have to develop technology based systems of transmission to potentially 26 other different systems of the other Member States.

Costs for carriers/competition in the internal market (0): National legislation obliging carriers to communicate PNR data to the relevant national authorities would mean that carriers collecting and processing this data would need to comply with the legal and technical requirements of each different system, regarding for example methods of transmission, data security standards for transmission of data, varying data formats amongst other. Considerable costs, as well as technical challenges, can be expected for carriers if they would have to respond to multiple requirements which differ substantially from one another. Since each Member State would be left to regulate the issue of access to PNR data domestically, it is not unlikely that such solutions will not comply with the 'single window' approach, i.e. that there should only be one authority in each Member State requesting data from the carriers**.** This would lead to a sharp increase in the costs for carriers as they would need to establish and keep secure communication channels with each different authority. In addition, in case some but not all Member States choose to develop their own PNR data collection and transfer systems, carriers operating predominantly from Member States which do not have PNR data legislation might be in an advantageous position compared to carriers in countries that do.

Encouraging a global approach (0): It is anticipated that more third countries will request the provision of PNR data from the Union. Even though the Communication on the global approach to the transfer of PNR data to third countries encourages the Union to insist on certain standards and to ensure consistency in such bilateral agreements with third countries**,** these standards will have less impact if the EU is unwilling or unable to impose such standards on its own Member States. Under this option the EU would not take full advantage of the possibility of requesting reciprocal treatment from third countries with which the EU has an agreement. Currently the third countries with which the EU has signed PNR Agreements only undertake to share some analysis of PNR data with authorities of Member States. The Agreements do not go as far as requesting the third country to transmit all relevant flight data to the Member States to do their own analysis and processing.

5.2. Impacts of the options addressing the structure for collecting and processing PNR data (Policy Option B)

5.2.1. Decentralised collection and processing of data by Member States (Option B1)

Increasing security in the EU (+++): This option would potentially entail a faster transmission of the collected PNR data from a Passenger Information Unit designated in each Member State to the relevant competent law enforcement authorities, than under the EU Centralised Unit option. Fast transmission is important since it allows more time to process the data and identify high-risk passengers in advance of their arrival, especially in cases where tickets for travel were bought at the last minute. It further provides time for law enforcement authorities to organise their reaction when they are expecting the arrival of a wanted or suspected individual by setting up teams to make the arrest or organise surveillance. More importantly, as PNR data are usually processed on the basis of very sensitive information, like the assessment criteria and other law enforcement databases held by each Member States, our consultations showed that the Member States would

be more willing to use such sensitive information under the auspices of their own national systems than with an EU Centralised Unit, thus rendering the processing of PNR data much more effective and contributing to increasing security in the EU quite substantially. There is a risk, however, that the Passenger Information Units of the Member States would apply diverging criteria in assessing passengers, leading to the risk that the same passenger is identified in one Member State but not in another. This could be remedied with the establishment of guidelines at the EU level on how passengers should be assessed. Such guidelines could be in the form of best practices on how the assessment of passengers should be carried out, resulting from an advisory comitology procedure. It would of course be essential that the actual assessment of passengers is carried out by each Member State separately as each would have different information on the basis of which to make its assessments.

Protection of personal data (--): Under this option the transmitted data would remain within one Member State and only the PNR data of identified passengers would be transmitted to other Member States. The data of passengers would be processed only by the Member State from which the passenger arrives or departs rather than by other Member States irrelevant to the person's travel. It would also involve the processing of the passenger's data only on the basis of data available in the specific Member State rather than against any information that might exist about the passenger elsewhere in the EU. Furthermore, it would be clear which Member State will be responsible for implementing the passenger's data protection rights and the passenger would know where to seek redress in the event of any violation of such rights.

Costs on public authorities (--): The option of creating Passenger Information Units in each Member State would entail costs which would 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. The costs for establishing the system would be substantial because each Member State would have to set up or designate 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. Because the setting-up and operation of such a Unit involves substantial costs, it should be possible for two or more Member States to establish or designate the same Passenger Information Unit to receive, filter, process and forward the data. This would be especially helpful to Member States with few international flights or which do not face a severe threat to their security or serious problems with serious crime.

Costs on carriers/competition in the internal market (--): 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 (as opposed to the cost of "pulling" data which is estimated at around 0,03 Euro per passenger). The carriers would also have to bear the one-off cost of setting-up the system (hardware and software), as well as recurring costs such as, personnel and maintenance costs. It should be noted that the software for carrying out transmissions of data by "push" and "pull" methods, have already been developed and therefore the cost of purchasing such software would be considerably less that some years ago. Furthermore, as PNR data are more often used in third

countries than before, new software developers have entered the market, which until some years ago was dominated by fewer companies. This has led to substantial reduction in costs. The carriers would also need to establish communication channels with each Passenger Information Unit in order to transmit the relevant data to each Member State. This option would provide carriers with a 'single window' in each Member State rather than having several different authorities in each Member State requesting data from the carriers.

Encouraging a global approach (+++): It is anticipated that an increasing number of third countries will request PNR data from the EU. This option would provide the EU with the ability to insist on certain standards and to ensure consistency in bilateral agreements with third countries. It would also make it possible to request reciprocal treatment from third countries with which the EU has already concluded an agreement, something that is not currently possible. Together with the Communication on the global approach to transfers of PNR data to third countries, this would allow the EU to encourage a global approach on the use of PNR data. Because the use of PNR data requires specific action from non-EU carriers, it is possible that the third countries where such carriers are based will react by introducing similar measures or by refusing to provide such data unless bilateral agreements are concluded with the EU. This is however considered unlikely because the experience with countries that use PNR data shows quite clearly that, despite their national measures which affect carriers worldwide, no retaliation has been recorded from another country. 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 the use of PNR data is currently only undertaken by those countries that consider such an investment necessary to enhance their internal security. As a result, 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 offered by the proposed measure to increase the internal security of the EU.

5.2.2. Centralised collection and processing of data at EU level (Option B2)

Increasing security in the EU (++): This option would ensure the application of common criteria for identification of passengers and would make it possible to identify travel patterns and behavioural characteristics more accurately because they would be based on PNR data for the whole of the EU. As such, the centralised collection of data would contribute substantially to increasing security in the EU. However, for the purpose of performing the assessment of the passengers, the responsible central authority would have to gather information from all the Member States. Such information would have to be up-to-date at all times, and the processing system would have to be fed with information on a 24/7 basis because of the number of flights entering and leaving the Union. 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 assessments of passengers. Such direct access is considered highly sensitive by the Member States and the consultations with the Member States indicated that they would be very reluctant to exchange such information and give direct access. Member States' reluctance to this option could result in practical problems in the implementation of the system and a high probability of failure, thereby reducing/obstructing/impeding substantially the positive impact that the measure is expected to have on security.

Protection of personal data (--): The advantage of having an EU Centralised Unit to collect, process and retain the data is that it might be in a better position to ensure that the data is transmitted and used within the uniform safeguards and redress mechanisms for the data subjects. This might ultimately involve less interference with the right to data protection of passengers. It would also ensure that exactly the same rules apply to all passengers. Furthermore, the data for each passenger will be assessed on the basis of information from all Member States, irrespective of where the passenger arrives or departs from. Such extensive processing would, however, be very cumbersome and outweigh the other advantages of having an EU Centralised Unit.

Costs on public authorities (-): Under this option, the costs would be borne by the EU budget and as a result, the Member States would not have to bear any costs as they would not have to develop their own Passenger Information Unit. The costs of setting up an EU Centralised Unit would be very high because such a Unit would receive the data and would therefore need to develop the necessary mechanisms for processing and transmitting the data to the relevant authorities. The mechanism developed would have to be of an especially high capacity in order to deal with the vast amounts of data from carriers and would be quite complicated. There is a high possibility that such a system could be subject to frequent crashes because of the vast amount of data and there is therefore a risk that it would be unworkable. A centralised system can be distinguished from systems such as the Schengen Information System (SIS) and the Visa Information System (VIS) because the volume of data which will be entered into such a system will be substantially bigger than that 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 PNR 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 each year. Such figures are also expected to rise every year. In addition, an EU Centralised Unit would need to operate on a 24/7 basis and be staffed with officials requiring special training in order to be able to work with fact-based rules. The EU does not currently have the expertise or the capacity to establish such a Centralised Unit.

Costs on carriers/competition in the internal market (-): 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, (as opposed to the cost of "pulling" data which is estimated at around 0,03 Euro per passenger). The carriers would also have to bear the one-off cost of setting-up the system for "pushing" or "pulling" (hardware and software), as well as recurring costs of personnel and maintenance.. This option would provide carriers with a 'single window' for the whole of the EU, i.e. they would need to establish secure communication channels for transmitting the data only with one authority for the whole of the EU rather than different authorities in each Member State. This would be very beneficial to the carriers from a financial point of view.

Encouraging a global approach (+++): The impacts are the same as those described above for option B1.

5.3. Impacts of the options addressing the purpose limitation of the proposed measures (Policy Option C)

5.3.1. Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime only (Option C1)

Increasing security in the EU (++): The use of PNR data exclusively for the prevention, detection, investigation and prosecution of terrorist offences and serious crime would have a very positive impact on increasing security in the EU. Terrorism and other serious crime are the biggest threats to security. By making PNR data available for the prevention, detection, investigation and prosecution of such crimes, law enforcement authorities will be provided with a necessary tool for the efficient performance of their tasks.

Protection of personal data (--): Limiting the measure to the prevention, detection, investigation and prosecution of terrorist offences and serious crime would involve the processing of PNR data only for the narrower possible purposes. The use of that data would be authorised only for purposes for which no other tool would be able to fulfil the same objectives.

Costs on public authorities (--): Restricting the use of the data to the prevention, detection, investigation and prosecution of terrorist offences and serious crime would involve a limited and specifically targeted group of authorities using the data. This would have cost advantages, as it would not be necessary to build secure connections for the exchange of the data between more authorities or to connect the national PNR database with additional databases on visas and aviation security amongst others. Extending the purpose beyond the abovementioned would lead to greater costs.

Costs on carriers/competition in the internal market (--): Both the option of using the data exclusively for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and the option of using it for further purposes would have the same impacts as regards the costs on the carriers and the competition in the internal market.

Encouraging a global approach (+++): Limiting the measure to law enforcement purposes would be in line with the general international approach of the EU towards third countries on PNR which only refer to such purposes and would allow the EU to set up its own standards to be promoted at international level.

5.3.2. Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and other policy objectives (Option C2)

Increasing security in the EU (+++): Extending the scope of the use of PNR data for other purposes could be considered useful, especially regarding the use of such data in the fight against irregular immigration, aviation security and health safety. However, other less intrusive instruments would be preferable for addressing those concerns, such as the use of API data. There is currently no clear and direct need to use PNR data for these purposes.

Protection of personal data (---): Although extending the use of PNR data to other purposes would be very useful, it cannot be justified as necessary. Other, less intrusive measures would be

more appropriate for these purposes. Moreover, under this option, more authorities would have the right to use the data which would require additional safeguards in order to comply with data protection principles.

Costs on public authorities (---): If extension of the use of PNR data is extended to purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime this will lead to a substantial increase in costs for public authorities.

Costs on carriers/competition in the internal market (--): The impacts are the same as those described above for option C1.

Encouraging a global approach (-): Extending the use of PNR data to purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime, would be inconsistent with current practice as it would go further in its domestic PNR system than the approach taken for third countries. .

5.4. Impacts of the options addressing the modes of transport to be covered by the proposed measures (Policy Option D)

5.4.1. Air carriers only (Option D1)

Increasing security in the EU (++): Even if the use of PNR data is limited to travel by air, it would contribute towards a substantial increase of the internal security in the EU. Air travel is the most common mode of transport for travelling to and from the EU territory from the majority of third countries. Due to its speed, it represents the most attractive mode of transport. As a result, even if any future measure is limited to air travel a high percentage of travellers would be covered by it. Further, because of the dramatic effects of a plane crash, and because of the destruction caused by such a crash, terrorists appear to have a preference for using aircraft to perform an act of terror. In addition, criminals who traffic people and goods also tend to use air travel because it is faster than other modes of transport. However, under this option not all controlled border crossings to the EU would be covered, and there would therefore continue to be a high possibility of terrorists and criminals entering its territory via other border crossings/land or sea borders. Furthermore, there remains a risk that those wishing to enter EU territory use alternative means of transport, for example ship, ferry, train, bus, thus making the instrument less effective. However, overall, this option could sufficiently achieve the goal of increasing security in the EU as a measure covering all flights to and from any third country would ensure that the Member States authorities are given sufficient tools for identifying when a potential suspect will attempt to enter the territory of the EU and will allow the analysis the data over a given period of time of relevance for the assessment criteria.

Protection of personal data (--): Limiting the use of PNR data to travel by air would involve collecting and processing of data of air passengers only, thereby limiting the interference with the passengers' right to the protection of their personal data. In addition, it is important to note that

air carriers already collect and store these data for quite long periods for commercial purposes[49]; this option would therefore not lead to the collection of any new data.

Costs on public authorities (--): This option would involve fewer costs than the extension of the use of PNR data to air, sea and rail carriers because it would involve collection, processing and retention of less data and fewer connections with carriers to obtain this data

Costs on carriers/competition in the internal market (--): Because air carriers are the only transport providers that already have mechanisms to collect PNR data of passengers developed and used for commercial purposes, the restriction of the use of PNR data to air carriers only would not lead to heavy costs for air carriers**.** However, it should be noted that the distinction between air and other forms of travel, leads to a possibility that air carriers are put at a competitive disadvantage as they would have to incur costs to comply with the system that other carriers will not have to do. This could lead to a distortion of competition in the EU. However, this would depend on which air routes are considered to be in competition with non-air routes, and which markets are considered to be separate.

Encouraging a global approach (+++): Restricting the use of PNR data to air carriers only would be in line with the general international approach and the agreements that the EU signed with third countries on PNR data which only refer to air travel.

5.4.2. Air, sea and rail carriers (Option D2)

Increasing security in the EU (+++): Any measure covering air, sea and rail travel would ensure that all (other than road) border crossings are covered and would therefore limit the possibility of having security gaps, thereby increasing security in the EU.

Protection of personal data (---): Extending the use of PNR data to sea and rail travel would lead to the collection and processing of more data because these carriers do not currently collect such data. In any case it would lead to the collection of more data than under Policy Option D1.

Costs on public authorities (---): Extending the use of PNR data to all modes of transport would be more costly for public authorities than restricting it to air travel because it would involve more collection, processing and retention of data and more connections with carriers to obtain the data.

Costs on carriers/competition in the internal market (---): This option would entail substantial costs and administrative changes for non-air carriers because they would have to set up such data collection and transfer mechanisms from scratch and change their operational systems substantially.

Encouraging a global approach (-): If the EU extends the use of PNR data to sea and rail travel, it would be going further for its domestic PNR system than it does for third countries. This approach would therefore not be consistent with existing practice.

[49] The retention periods by carriers vary substantially and sometimes reach 40 years

6. COMPARING THE OPTIONS

Policy Option A on maintaining the status quo presents very limited advantages on increasing the security of the EU, but otherwise would have very negative impacts. Bearing in mind the direction in which this policy field is currently developing, it is anticipated that it would have negative impacts in the sense of creating administrative difficulties for the public authorities stemming from numerous diverging national systems. The costs of compliance with potentially 27 diverging systems would be huge, for both the public authorities and the carriers. Security benefits would be limited, since there would be no harmonisation of the various aspects of the national systems for the exchange and use of PNR data. In addition, the development of different legal frameworks and mechanisms in the different Member States presents more possibilities for intrusive interferences to the data protection principles because it would lead to diverging standards of data protection in each Member State. Moreover, such an option would not be consistent with the Union policy as regards agreements on PNR with third countries.

The options under Policy Options B aim to address the structure of the system needed to regulate the use of PNR data. Whether through a centralised or a decentralised system, taking action at the EU level is preferable to refraining from taking any action because it presents the clear advantage of significantly increasing security in the EU. Regarding the structure of any system to collect and process PNR data, the decentralised collection of data (Option B1) presents advantages over the centralised collection of such data (Option B2). The option of centralised collection of data would have a high possibility of failure because it could not guarantee adequate co-operation between the Member States and at a practical level the system would be cumbersome and costly to operate due to the enormous amount of data that it would have to process and retain. Policy Option B1 would be more costly, for both the public authorities and the carriers compared with Policy Option B2**.** The advantages, however, for security outweigh the disadvantages in terms of costs, since increasing security is the primary aim of the proposed measure. Both options would have the same impacts on the protection of personal data and on encouraging a global approach.

Concerning the purpose limitation of any future measures, Policy Option C2 whereby the scope of the proposed measure would be extended to purposes other than the prevention, detection, investigation and prosecution of terrorist offences and serious crime presents some advantages for security compared with Policy Option C1. However, it also involves substantially more interference with data protection and more costs for the public authorities than Policy Option C1 which would allow the use of PNR data exclusively for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Moreover, Policy Option C2 presents fewer opportunities in terms of encouraging a global approach than Policy Option C1 since it would go further than the policy of the EU on PNR agreements with third countries. On this basis, Policy Option C2 on extending the use of PNR data to other purposes seems to be disproportionate at this stage.

Regarding the options in relation to the modes of transport that should be covered by any future measure, Policy Option D2 whereby the proposed measure would be extended to air, sea and rail carriers presents some advantages for security compared with Policy Option D1 as it would cover more modes of transport and more passengers. However, it involves substantially more interference with data protection and more costs for the public authorities and the carriers than

Policy Option D1 under which the measure would be applied exclusively to air carriers. Moreover, Policy Option D2 presents fewer advantages in terms of encouraging a global approach since it would go further than the policy of the EU on PNR agreements with third countries. In addition, the idea behind using PNR data is simply to obtain access to the data that is already collected by carriers. Since most train and ships/ferry carriers do not normally collect such data, it would be disproportionate at this stage to require them to transmit data to public authorities. On the basis of the above, Policy Option D2 on extending the scope of the measure to cover sea and rail travel seems to be premature, at least at this stage. Such an extension to sea and rail travel could be considered in the future, once we will have learned from the experiences with PNR collection from air travel.

Summary table of the impacts of the policy options

Impacts of policy options	Status quo	Options addressing structure for collecting and processing PNR		Options addressing purpose limitation of PNR		Options addressing modes of transport covered by PNR	
	Policy Option A **Status quo**	**Policy Option B1** **Decentra-lised PNR system at MS level**	**Policy Option B2** **Centralised PNR system at EU level**	**Policy Option C1** **Terrorist offences and serious crime**	**Policy Option C2** **Terrorist offences and serious crime and other policy objectives**	**Policy Option D1** **Air carriers**	**Policy Option D2** **Air, sea and rail carriers**
Increase security in the EU	0	+++	++	++	+++	++	+++
Protection of personal data	0	--	--	--	---	--	---
Costs on public authorities	0	--	-	--	---	--	---
Costs on carriers / competition in the internal market	0	--	-	--	--	--	---
Encouraging a global approach	0	+++	+++	+++	-	+++	-
Preferred policy option		√		√		√	

7. PREFERRED POLICY OPTION

7.1. Analysis of the 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 for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and other serious crime seems to be the best policy option (combination of Policy Options B1, C1 and D1). This option would be preferable since it would provide better means of increasing security in the EU, while at the same time ensuring that interference with the protection of personal data is kept to a minimum and that costs are kept at an acceptable level. It should be noted that this option it is not believed to present the ultimate solution to the problem but, at the current stage, it is the most desirable solution. It is a good starting point and will help towards gathering experience in this field. In any event an EU instrument on the use of PNR data should be evaluated after a reasonable period of time to assess its implementation. It should be noted that the preferred option will not have an impact on the EU budget.

The structure of the system should be decentralised. This option would have more benefits for the security in the EU since any centralised system, because of the nature of PNR data processing, would risk failing. Even though the centralised option involves fewer costs than the decentralised option, the advantage to security, which is the main purpose of the measure, would outweigh the costs element.

The purpose of any future measure should be limited only to the prevention, detection, investigation and prosecution of terrorist offences and serious crime rather than be extended to other purposes such as health safety, aviation security, immigration for instance. The negative impact this would have on the protection of personal data, costs and encouraging a global approach to PNR data outweigh the advantages to increased security this purpose extension would bring.

As a first step, it seems more proportionate that the proposal is limited to air carriers. Even though an extension to other modes of transport would have benefits for security, it would involve more costs for the public authorities and the carriers and more interference with data protection.

The EU needs to act as soon as possible in this area in order to reduce the possibility of various diverging 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.

7.2. Costs of the preferred option

An analysis of the costs of the preferred policy option appears in detail in **Annex A** and corresponds to the analysis carried out for the purposes of the 2007 Impact Assessment. The costs are differentiated between costs for public authorities and costs for carriers. This analysis did not

elicit any comment from either the Member States or the air carriers at the time of publication of the 2007 Impact Assessment. According to the 2007 calculations, the overall cost of the preferred option for public authorities and carriers would be as follows:

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

Set-up cost (non-recurring cost)	€ 614 833 187
BUT assuming an amortisation period of five years	€ 122 966 637
Annual personnel costs (recurring)	€ 11 686 749
Annual maintenance costs (recurring)	€ 61 483 319

In relation to all EU carriers together, such costs are:

Set-up cost for PUSH (non-recurring costs)	€ 11 647 116
BUT assuming an amortisation period of five years	€ 2 329 423
Transmission costs for PUSH twice per passenger (recurring)	€ 2 250 080
Personnel and maintenance costs (recurring)	€ 5 435 321

Following the 2007 Impact Assessment, the Commission published a tender for a study on ways of setting up an EU network for exchanging PNR data. The report 'Study on ways of setting up an EU network on exchange of Passenger Name Record (PNR) data for law enforcement purposes'[50] was issued in 2009 and includes a new assessment of the costs.

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

Set-up cost (non-recurring cost)

5 large Member States * € 25 million = € 125 million

15 medium-sized Member States* € 5 million = € 75 million

7 small Member States* € 3 million = € 21 million	€ 221 000 000
BUT assuming an amortisation period of five years	€ 44 200 000
Annual personnel costs (recurring)[51]	€ 11 686 749
Annual maintenance costs (recurring)[52]	€ 61 483 319

[50] Authors: Accenture and SITA.

[51] These costs were not re-assessed under the Accenture study. The 2007 figures are therefore maintained.

[52] Ditto.

In relation to all EU carriers together, such costs are:

Set-up cost for PUSH (non-recurring costs)[53]

€100 000 * 120 EU-based carriers = €12 000 000

€100 000 * 80 non-EU-based carriers[54] = €8 000 000

BUT assuming an amortisation period of five years €4 000 000

Transmission costs for PUSH twice per passenger (recurring)

€33 500 per airline per year*120 carriers*3connections*2 PUSH €24 120 000

Personnel/maintenance costs (recurring) €6 240 000

The 2009 figures indicate a decrease in costs for public authorities to set up an EU PNR system but an increase in costs for carriers in comparison with the cost calculation performed in 2007. The actual costs will be somewhere in between these two assessments and, at least as regards the costs to carriers, most likely closer to the 2007 assessments, which are based on the market prices taken directly from carriers.

It is important to note that, even with the very high calculations of 2009, if the carriers decide to pass on their costs to passengers, this would result in a surcharge of less than €0.10 per ticket, a negligible amount in relation to the overall ticket price.

8. MONITORING AND EVALUATION

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

Each Member State could prepare and transmit to the Commission an annual report on the implementation of the systems containing information on the following indicators:

– volumes of data received,

– cases which have ended in successful identifications of suspects,

– number and type of case where retained data were used for investigations,

– cases where data were exchanged with other Member States and third countries,

---

[53] The costs for PULL have not been assessed under the study, as it had become obvious at that stage of the negotiations between stakeholders that this would not be an acceptable option. It is, however, clear from Annex A that the costs of PULL would be substantially less than the costs of PUSH.

[54] It is noted that the costs for non-EU-based carriers were not assessed for the purposes of the 2007 Impact Assessment.

– number of cases of redress related to data protection and their outcome.

The Commission should assess the operation of the Directive within four years from its entry into force and submit a report to the Parliament and the Council. This should evaluate whether the use of PNR data has met its objectives and whether Member States have complied with their obligations. The review should also examine whether the system has been successful and substantiate its conclusions with statistics. The review should also take into account the annual reports of the Member States and consider all matters arising there from.

The Commission should also consider the possibility of extending the measure to internal EU flights within two years from its entry into force. This would provide the opportunity to have a transitional period and to gain experience from the functioning of first PNR data Directive.

ANNEX A – TABLE OF ECONOMIC IMPACTS OF PREFERRED OPTION

Proposal On A Common Approach to the Use of Passenger Name Records (PNR) Data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime **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 the prevention, detection, investigation and prosecution of terrorist offences and serious crime 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 data 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 method.		
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 employment 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	