EUROPEAN COMMISSION

Brussels, 2.2.2011
SEC(2011) 133 final

COMMISSION STAFF WORKING PAPER

SUMMARY OF THE 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) 132 final}

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

On 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes[1]. The proposal was accompanied by an Impact Assessment[2]. The proposal was extensively discussed in the Council working groups and the progress made in the discussions was endorsed by the JHA Council in 2008. The discussions on the proposal in the working groups allowed consensus to be reached on most of the provisions of the proposal.

Upon entry into force of the Treaty of Lisbon on 1 December 2009, the Commission proposal, not yet adopted by the Council by that date, became obsolete. 'The Stockholm Programme — An open and secure Europe serving and protecting the citizens'[3] calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

For the 2007 Impact Assessment, the Commission consulted all the stakeholders. Following the adoption of the Commission's 2007 proposal, all stakeholders, namely the European Parliament, the Article 29 Data Protection Working Party, the European Data Protection Supervisor, the Fundamental Rights Agency and airline associations, published their positions on it. The purpose of this report is to examine the possibility of adopting a new proposal to replace the 2007 proposal under the provisions and procedures of the Lisbon Treaty It aims to answer criticisms raised by the stakeholders and include all new facts and experience gained since 2007.

2. PROBLEM DEFINITION

2.1. Threat of terrorism and serious crime

Over the last decade the European Union and other parts of the world have experienced a spread of cross-border crime. 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. Europol's EU Organised Crime Threat Assessment 2009 found that most organised crime threats have an international dimension and that most serious organised crime involves international travel.

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. Europol's 'EU Terrorism Situation and Trend Report 2010', despite finding that terrorism decreased in the EU during 2009, stressed that the threat remains real and serious. Most terrorist campaigns, especially the type that Europol calls 'Islamist terrorism', have a transnational character.

2.2. PNR data and their uses

PNR data have been used for several years, mainly by customs and law enforcement authorities around the world. It is possible to use PNR data for police and judicial matters:

- **re-actively:** in investigations, prosecutions, unravelling of networks after a crime has been committed. In order to allow law enforcement authorities to go back in time far enough, a

1 COM(2007) 654.
2 SEC(2007) 1453.
3 Council document 17024/09, 2.12.2009.

commensurate period of retention of the data by law enforcement authorities is necessary in such cases;

- **in real time:** 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 who were previously 'unknown' to law enforcement authorities and for running the data against databases of persons and objects sought;
- **pro-actively:** 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 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,[4] 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.

---

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

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 led 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.

Arrangements for the transmission of PNR data in the context of the fight against terrorism and transnational organised crime have been concluded between the EU and the United States, Canada and Australia. It can be anticipated that more third countries are likely to request the provision of PNR data from air carriers operating flights from the EU.

The United Kingdom, France and Denmark have already enacted primary legislation for the capture and use of PNR data. Such national measures diverge in several respects and it is likely that once the complete regulatory framework in these Member States is adopted, there will be further divergence. As more Member States are preparing their own PNR legislation, up to 27 considerably diverging systems could be created, resulting in uneven levels of data protection, security gaps, increased costs and legal uncertainty for carriers.

2.3. EU right to act and subsidiarity

The right of the EU to act in this field is enshrined in Articles 82 and 87 in Title V of Chapter V of the Treaty on the Functioning of the European Union. As most of the categories of serious crimes, such as drugs and human trafficking, include international travel at some stage, it is essential that authorities collect, process and exchange PNR data for increasing the internal security of the EU. Because of the free circulation of persons in the Schengen area, it is necessary for all Member States to use PNR data, in order to avoid security gaps. In addition, action at EU level will ensure harmonised provisions on safeguarding data protection, reduced costs and legal certainty for the carriers.

3. OBJECTIVES

3.1. Policy objectives

The general objective is to increase the internal security of the EU, while respecting the right to protection of personal data and other fundamental rights, with 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 and avoiding security gaps.

(2) To ensure that individuals' right to the protection of their personal data is duly respected when PNR data are collected and processed by facilitating the exchange of

PNR data among responsible authorities and ensuring that access to PNR data is limited to what is necessary.

(3) To provide legal certainty to and reduce costs for carriers by reducing differences in legal and technical requirements imposed on carriers.

3.2. Fundamental rights considerations

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[5].

The use of PNR data would interfere with the fundamental rights to the protection of private life and to the protection of personal data. This may be made subject to limitations and conditions, provided such interference is carried out 'in accordance with the law' and is 'necessary in a democratic society'. As the proposed actions aim to combat terrorism and other serious crime, they would serve an objective of general interest able to justify such limitations, subject to the principle of proportionality.

Any proposed action would fall within the scope of Title V of Chapter V TFEU on police cooperation. The Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[6] would only apply to those aspects of any proposed action where some personal data would be transmitted between Member States and therefore leave a gap for personal data processed at national level only. There are currently no EU rules regulating such processing of personal data at national level. The most suitable solution would be that the data protection safeguards of any proposed measure are in line with the Framework Decision 2008/977/JHA. This would guarantee a uniform standard of protection of personal data.

A commensurate period during which the data are retained by the relevant authorities is necessary. On the method of transmission of the data by the carriers, the advantages of the 'push' system over the 'pull' system are indisputable, and therefore the 'push' system should apply for all transmissions.

As regards criticisms of 'profiling', EU data protection laws grant every individual the right not to be subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate personal aspects relating to him/her. Any automated individual decision should be fully verified and confirmed by a human being and comprise arrangements allowing the data subject to put his or her point of view.

4. POLICY OPTIONS

The Impact Assessment examines four main options.

Option A. Refraining from addressing the issue at EU level and maintaining the status quo.

Option B. Options addressing the structure of the PNR system:

B.1: Decentralised collection and processing of data by Member States; B.2: Centralised collection and processing of data at EU level.

---

5 COM(2010) 573, 19.10.2010

6 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).

Option C. Options on the limitation of the purpose:

C.1: Access for terrorist offences and serious crime only; C.2: Access for terrorist offences and serious crime and other policy objectives.

Option D. Options on the modes of transport:

D.1: Air carriers only; D.2: Air, sea and rail carriers.

Option E. Voluntary/enhanced cooperation. This option of encouraging cooperation between the Member States in the field was rejected at the initial stage.

5. COMPARISON OF POLICY OPTIONS AND THEIR IMPACTS

The options were assessed in relation to their impacts in terms of increasing security in the EU, increasing the protection of personal data, costs for public authorities, costs for carriers/competition in the internal market, relations with third countries, and encouraging a global approach.

Option A on maintaining the status quo presents limited advantages with respect to increasing the security of the EU, but otherwise has negative impacts, in the sense of creating administrative difficulties and costs stemming from numerous diverging national systems.

On Option B, the decentralised collection of data (Option B1) presents advantages over the centralised collection of such data (Option B2) in relation to increasing the security of the EU. The option of centralised collection of data would have a high risk of failure because it cannot guarantee adequate cooperation between the Member States and at a practical level the system would be cumbersome and costly to operate. Option B1 would be more costly compared with Option B2. However, the advantages for security outweigh the disadvantages in terms of costs.

On purpose limitation, Option C2 presents some advantages for security compared with Option C1, but involves substantially more interference with data protection and more costs than Option C1. Option C2 on extending the use of PNR data to other purposes seems disproportionate at this stage.

On the modes of transport, Option D2 presents advantages for security compared with Option D1 as it would cover more modes of transport and more passengers, but involves more interference with data protection and more costs than Option D1, under which the measure would be applied exclusively to air carriers. Option D2 on extending the scope of the measure to cover sea and rail travel seems premature, at least at this stage.

6. PREFERRED OPTION

The creation of a new legislative proposal applicable to travel by air with 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 at this stage (combination of Options B1, C1 and D1). It would provide better means of increasing security in the EU, while ensuring that interference with data protection is kept to a minimum and that costs are kept at an acceptable level.

An analysis of the costs of the preferred policy option was carried out for the purposes 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)	€614833187
BUT assuming an amortisation period of five years	€122966637
Annual personnel costs (recurring)	€11686749
Annual maintenance costs (recurring)	€61483319
In relation to all EU carriers together, such costs are:	
Set-up cost for PUSH (non-recurring)	€11647116
BUT assuming an amortisation period of five years	€2329423
Transmission costs for PUSH twice per passenger (recurring)	€2250080
Personnel and maintenance costs (recurring)	€5435321

In 2008 the Commission published a tender for a study on ways of setting up an EU PNR network. The report 'Study on ways of setting up an EU network on exchange of Passenger Name Record (PNR) data for law enforcement purposes'[7] 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)	€221000000
BUT assuming an amortisation period of five years	€44200000
Annual personnel costs (recurring)	€11686749
Annual maintenance costs (recurring)	€61483319
In relation to carriers together, such costs are:	
Set-up cost for PUSH (non-recurring)	
€100000 * 120 EU-based carriers =	€12000000
€100000 * 80 non-EU-based carriers =	€8000000
BUT assuming an amortisation period of five years	€4000000
Transmission costs for PUSH twice per passenger (recurring)	
€33500 per airline per year*120 carriers*3connections*2 PUSH	€24120000
Personnel/maintenance costs (recurring)	€6240000

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.

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 price of tickets.

[7] Authors: Accenture and SITA.

7. MONITORING AND EVALUATION

Each Member State could prepare an annual report on the implementation of the systems. The Commission should assess the operation of the Directive within four years from its entry into force to monitor whether the use of PNR data has met its objectives, whether Member States have complied with their obligations and whether the system has been successful.

The Commission should also consider the possibility of extending the measure to internal EU flights. This would provide the opportunity to have a transitional period and gain experience from the functioning of the first PNR Directive.