COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2007
SEC(2007) 1422

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

COUNCIL FRAMEWORK DECISION

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

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2007) 654 final}
{SEC(2007) 1453}

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

The European Council in its Declaration on combating terrorism of March 2004 called on the European Commission to bring forward a proposal "*for a common EU approach to the use of passengers' data for border and aviation security and other law enforcement purposes*". A European policy in this area has been announced in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003. The request for European action on PNR was repeated by the European Council on several occasions.

The Commission services held extensive consultations of the relevant stakeholders, namely the Member States, the national data protection authorities of the Member States, the EDPS, the Air Transport Association of America, the International Air Carrier Association, the Association of European Airlines, the European Regions Airline Association and the International Air Transport Association.

The choice of dealing with the issue by means of encouraging cooperation between the Member States was one which was considered initially but rejected. Such cooperation could be in the form of exchange of best practices, but it is considered that such an option would not achieve the desired objectives of increasing security and would be ultimately very costly.

2. PROBLEM DEFINITION

Terrorism currently constitutes one of the greatest threats to security, peace, stability, democracy and fundamental rights, values on which the European Union is founded, as well as a direct threat to European citizens. The threat of terrorism is not restricted to specific geographic zones. Over the last few years the European Union and the world have experienced more than ever before its geographic spread. Criminals have taken full advantage of the effects of globalisation and are using more and more opportunities to travel, exchange information and communication to perform their business. The Member States of the EU are realising more and more the need to raise their level of awareness of this threat. At this point, it seems appropriate to proceed with the introduction of PNR legislation and the Member States indicate that there is a strong need for the EU to take proactive, rather than solely reactive, measures in order to combat terrorism and serious crime effectively.

This impact assessment aims to assess whether there is a need for a proposal at European Union level aimed at setting up a coherent legal framework regarding the obligation of carriers to transmit PNR data to the relevant competent authorities for the purposes of preventing and fighting terrorist offences and organised crime. Such a measure would aim to contribute towards building intelligence about terrorists and criminals and to identifying behaviour patterns of such persons.

Air carriers have an obligation to communicate Advance Passenger Information (API) to the competent authorities of the Member States, under Council Directive 2004/82/EC[1], which are used for fighting illegal immigration. Further, those authorities may obtain the information which is contained in the PNR data of a passenger of an international flight by looking at his

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

ticket and the boarding card that he is required to fill in for the purpose of border control. The added value of the proposal is that the competent authorities of the Member States are able to receive the data in an electronic form and well in advance of a flight's arrival. This will provide the authorities with the possibility of processing it electronically and in substantially less time than if it were done manually. This, in turn, is beneficial for the authorities and the passengers since it reduces border control time.

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

- Running PNR data against alert systems in order to identify known terrorists and criminals.

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

- Running PNR data against a combination of characteristics and behavioural patterns, aimed at creating a risk-assessment. When a passenger fits within a certain risk-assessment, he could be identified as a high-risk passenger.

- Running PNR data against risk intelligence relevant at a certain time, with the aim of identifying high-risk passengers. For example, when intelligence exists that a travel agency in a certain country has connections with a specific terrorist organisation or criminal group, PNR data helps identify which passengers have bought tickets from such suspected agency.

- Providing intelligence on travel patterns and associations after a terrorist offence has been committed.

The rationale behind identifying unknown high-risk passengers is that this allows for secondary screening upon their arrival and further questioning by security officers and in specific circumstances, in combination with other information, to a refusal of entry in the territory of the destination country. At the same time it allows to reduce border controls for all other passengers.

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 and Canada and are limited to travel by air. 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, and are in the process of considering secondary legislation to implement national PNR systems. Such national measures are diverging on several aspects.

Other aspects of the problem include the sufficient protection of PNR personal data, as well the facilitation of border controls which are increasingly becoming a problem because of the large volumes of passengers. The electronic collection and use of PNR data will contribute towards managing this problem more efficiently. The possibility of performing security

controls on a traveller's PNR data before arrival in the country of destination, will fasten clearance of travellers at the border.

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

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

3. POLICY OPTIONS

The proposed actions involve the collection, processing, exchange and use of some personal data of citizens travelling to and from the EU. As such, they might interfere with the right to the protection of private and family life and to the protection of personal data as protected by the Charter on Fundamental Rights of the European Union and the European Convention of Human Rights. The right to private and family life however is not absolute, but subject to exceptions for reasons necessary "in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others", provided interference is done "in accordance with the law" and is "necessary in a democratic society". As the proposed actions aim to combat terrorism and organised crime, they would clearly come under the umbrella of the exceptions.

The measure would come under Title VI TEU. Until the time of drafting of the present impact assessment, the Commission Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters has not yet been adopted. In view of this, the aim should be to observe the data protection standards as set in European instruments, such as the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe. In practice, all Member States should also already have national legislation in place to cover data processing by law enforcement authorities.

The aims of the proposal will be:

- Fighting terrorist offences and organised crime by using PNR data and protecting citizens' life and physical integrity, the EU as a whole and each Member State,

- Providing legal certainty to carriers in terms of the legal requirements imposed upon them, while avoiding a distortion of the internal market through diverging legal requirements,

- Protecting citizens' fundamental rights, in particular the right to privacy, while recognising the need for a wider sharing of relevant personal data for law enforcement purposes,

- Developing an EU position in this area with the aim to encourage a global approach to the use of passenger data in the fight against terrorist offences and organised crime.

The Impact Assessment examines two main options with a number of variables – the no change option and the option of a legislative proposal.

The option of a legislative proposal is divided into two sub-options – a decentralised and a centralised collection of data for air travel.

The options were assessed in relation to their impacts on security in the EU, protection of privacy, costs for carriers, costs for public authorities, relations with third countries, competition in the internal market and convenience to passengers.

The Impact Assessment concluded that the preferred option is a legislative proposal with a decentralised system for data processing. The "no action" policy option does not present any real strength in improving security in the EU. On the contrary, it is anticipated that, bearing in mind the way that this field is currently developing, it will have negative impacts in the sense of creating administrative difficulties stemming from numerous diverging systems, increased costs of compliance with such diverging systems and distorting competition.

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

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

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

4. PREFERRED OPTION

The preferred option suggests a new legislative proposal applicable to travel by air with a decentralised collection of data as the best policy option. This option would provide better means of increasing security in the EU, while at the same time ensuring the better protection of data and minimising the costs for its setup and operation. It should be noted that it is not believed that this option presents the ultimate solution to the problem but, at the current stage, it is the most feasible solution. It presents a good starting point and will help towards

gathering experience in this very new field. It is foreseen that this proposal will be evaluated and, if possible, extended to a wider application at a later stage. It should be left to the Member States to extend the scope of such proposal to other modes of transport at this point. Further, Member States should be able to conclude bilateral or multilateral agreements or arrangements for the purpose of enhancing or facilitating the provisions of such proposal.

The proposal should take the form of a Framework Decision under Title VI of the Treaty on European Union.

Moreover, the Impact Assessment examines the various other parameters of the preferred option. It concludes the following:

- *The scope of the proposal as regards the modes of transport*: the majority of the consulted parties agree that the scope of the proposal should be limited to air transport as a first step, with the possibility of extending it to other forms of transport at a later stage. This approach is generally based on the fact that air carriers already have systems with which they capture PNR data and it would therefore be easier for them to comply with the proposal.
- *The geographical scope of the proposal*: most parties consulted believe that the geographical scope should be limited to flights from third countries to the EU and from the EU to third countries. At this stage, it is thought disproportionate to extend the scope of the proposal to flights from one Member State to another Member State and to internal flights within a Member State.
- *The use of and purpose for collecting the PNR data*: The collection of PNR data should be used for the purposes of Title VI only, i.e. the prevention of and fight against terrorist offences and organised crime.
- *The data retention period*: It was commonly agreed that, for the system to be effective, the data need to be retained for a period of 5 years, unless they were used for a crime investigation or an intelligence operation.
- *The body receiving the PNR data*: A majority of the Member States are in favour of the idea that the data be received by a Passenger Information Unit which will be identified within each Member State, while other Member States are in favour of a centralised EU Unit which would receive data from carriers from all the Member States.
- *The method of data transmission*: The "push" method of transmission is preferred to the "pull" method by all parties consulted. The main difference is that in the "push" method, the data are being transmitted by the carrier to the national authority, whereas in the "pull" method the national authority obtains access to the reservation system of the carrier and takes the data.
- *Onward transfers of the PNR data*: Most of the consulted parties are in favour of the PNR data being transmitted to the national competent authorities and to the competent authorities of other Member States. Some Member States are in favour of the data being transmitted also to the competent authorities of third countries.
- *IT security*: For the purposes of security of data transmission, most parties agree that common encryption standards could be adopted to ensure such security.

The proposed measure would further include provisions for its monitoring and evaluation.