COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 6.11.2007
COM(2007) 654 final

2007/0237 (CNS)

Proposal for a

COUNCIL FRAMEWORK DECISION

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

(presented by the Commission)

{SEC(2007) 1422}
{SEC(2007) 1453}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

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

Since 9/11, law enforcement authorities around the world have come to realise the added value of collecting and analysing so-called PNR data in combating terrorism and organised crime. PNR data are related to travel movements, usually flights, and include passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences and other information. The PNR data of a certain passenger usually does not contain all PNR fields, but only those that are actually provided by the passenger at the time of the reservation and information received upon check-in and boarding. It must be noted that air carriers already capture the PNR data of passengers for their own commercial purposes, but that non-air carriers do not capture such data. The collection and analysis of PNR data allows the law enforcement authorities to identify high risk persons and to take appropriate measures.

Until now, only a limited number of Member State have adopted legislation to set up mechanisms to oblige air carriers to provide the relevant PNR data and to have such data analysed by the competent authorities. This means that the potential benefits of an EU wide scheme in preventing terrorism and organised crime are not fully realised.

- **General context**

Currently, 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. These require that air carriers, which were already capturing the PNR data of passengers for their own commercial purposes, are obliged to transmit these data to the competent authorities of the USA and Canada. On the basis of an exchange of information with these third countries, the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes. The EU has further been able to learn from the experiences of such third countries in the use of PNR data, as well as from the experience of the UK from its pilot project. More specifically, the UK was able to report numerous arrests, identification of human trafficking networks and gaining of valuable intelligence in relation to terrorism in the two years of the operation of its pilot project.

The European Council of 25-26 March 2004 invited the Commission to bring forward a proposal for a common EU approach to the use of passengers' data for law enforcement purposes. This invitation has been reiterated twice, namely on 4-5 November 2004 in The Hague Programme and at the extraordinary Council meeting of 13 July 2005. A European policy in this area had also been announced already in the Commission Communication "Transfer of Air Passenger Name Record (PNR) Data: A global EU approach" of 16 December 2003.

- **Existing provisions in the area of the proposal**

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

For the purposes of the fight against terrorism and organised crime, the information contained in the API data would be sufficient only for identifying known terrorists and criminals by using alert systems. API data are official data, as they stem from passports, and sufficiently accurate as to the identity of a person. On the other hand, PNR data contains more data elements and are available in advance of API data. Such data elements are a very important tool for carrying out risk assessments of the persons, for obtaining intelligence and for making associations between known and unknown people.

- **Consistency with the other policies and objectives of the Union**

The proposal is fully in line with the overall objective of creating an European area of freedom, security and justice. It also complies with fundamental rights provisions, particularly with respect to the protection of personal data and the privacy of the persons concerned.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

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

passenger data have been organised under the umbrella of the Forum on the prevention of transnational organised crime.

For the purposes of the preparation of this proposal, the Commission services further consulted all the relevant stakeholders by way of a questionnaire which was sent out in December 2006. Subsequently, the Commission invited member State representatives to a meeting in Brussels on the 2 February 2007, during which the representatives of the Member States had the opportunity to exchange their views.

The questionnaire was sent to:

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

Replies were received from 24 Member States; a joint reply was received from the national data protection authorities of the Member States. Replies were also received from the EDPS, the Air Transport Association of America, the International Air Carrier Association (IACA), the Association of European Airlines (AEA), the European Regions Airline Association (ERA), the International Air Transport Association (IATA), LOT Polish Airlines and Austrian Airlines.

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

Summary of responses and how they have been taken into account

The consultation process has had a major impact on shaping the legislative proposal. More specifically, such impact affected:

- The choice of the policy option: it became clear from the replies which were received to the questionnaire that most of the Member States are clearly in favour of a legislative instrument which would regulate a common EU approach on the matter. The Article 29 Working Party was not convinced of the necessity of such a proposal and is therefore opposed to the proposal, but it noted that once the necessity is established or several Member States would be considering the development of a national PNR systems, then harmonisation of such measures at an EU level should be preferred.

- The scope of the proposal as regards the modes of transport: the majority of the consulted parties agrees that the scope of the proposal should be limited to air transport.

- The geographical scope of the proposal: most parties consulted believe that the geographical scope of the proposal should be limited to flights from third countries to the EU and from the EU to third countries.

- The use of and purpose for collecting the PNR data: The collection of PNR data should be used for the purposes of the third pillar only, i.e. the prevention of and fight against terrorism and related crimes and other serious crimes, including transnational organised crime.

- The data retention period: It was commonly agreed that, for the system to be effective, the data need to be retained for a period of 5 years, unless they were used for a crime investigation or an intelligence operation.

- The body receiving the PNR data: The majority of the Member States is 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 air carriers from all the Member States.

- The method of data transmission: The "push" method of transmission is preferred to the "pull" method by all parties consulted. The main difference of the two methods is that in the "push" method, the data are being transmitted by the carrier to the national authority, whereas in the "pull" method the national authority obtains access to the reservation system of the air carrier and takes the data.

- The onward transfers of the PNR data: Most of the consulted parties are in favour of the PNR data being transmitted to the national competent authorities and to the competent authorities of other Member States. Some Member States are in favour of the data being transmitted also to the competent authorities of third countries.

- **Collection and use of expertise**

There was no need for external expertise.

- **Impact assessment**

For the Impact Assessment, two main options with a number of variables were examined - the no change option and the option of a legislative proposal. Additionally, at an early stage the option of encouraging co-operation between the Member States in this field was rejected, since it was considered that this option would not achieve the desired objectives. Some Member States had suggested to expand the scope of the proposal so that it would also cover sea and rail travel. This option was also rejected at an early stage due to considerations of costs and the lack of existing systems which collect the relevant data.

The Impact Assessment concluded that the preferred option is a legislative proposal with a decentralised system for processing the data. 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.

The legislative proposal policy option possesses the clear advantage of increasing security in the form of reducing the risk of terrorist attacks and of serious crimes and transnational organised crime being committed on the territory of the EU. Moreover, 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 persons 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 because of the vast amounts of data that a centralised unit would receive, the complications of the different types of processing being carried out. Further, for such a unit to be operable, it would need to have access to various national databases of all Member States.

With regard to the impact of the proposal on relations with third countries, it cannot be excluded that some countries may request reciprocal access to PNR data relating to flights from the EU to their territories, even though in practice such an eventuality is very remote. The Union's existing agreements on PNR data with the US and Canada foresee such reciprocal treatment which may be enforced automatically.

The Commission carried out an impact assessment listed in the Work Programme[1].

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposal aims to harmonise Member State's provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime. All processing of PNR data under the proposal will be governed by the Council Framework Decision (xx/xx) on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters.

- **Legal basis**

The Treaty on European Union, and in particular Article 29, Article 30(1)(b) and Article 34(2)(b).

- **Subsidiarity principle**

The subsidiarity principle applies to the action by the Union.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reasons.

[1] SEC(2007) 1453.

The main reason why action by Member States would not be sufficient to achieve the objectives is that it is impossible for the Member States alone to achieve appropriate harmonisation of legal obligations in this area to be imposed on all air carriers operating flights into or from the European Union.

Action by Member States alone would not achieve the Member States interest because they would not be assured of having the relevant PNR data made available to them by the authorities of other Member States - this can only be guaranteed by an EU wide scheme.

Union action will better achieve the objectives of the proposal for the following reasons.

Action by the EU will better achieve the objectives of the proposal because a harmonised approach makes it possible to ensure EU wide exchange of the relevant information. Also, it makes it possible to provide for a harmonised approach towards the outside world.

The qualitative indicator which demonstrates that the objective can be better achieved by the Union is a more effective action in the fight against terrorism and organised crime.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal complies with the proportionality principle for the following reasons.

The scope of the proposal is limited to those elements which require a harmonised EU approach - including the definition of the tasks of the PNR Units, the data elements which need to be collected, the purposes for which the information may be used, the communication of the data between the PNR units of the Member States, and the technical conditions for such communication.

The proposed action is a Framework Decision which leaves as much scope as possible to the national decision makers. Also, the choice for a decentralised system means that the member States have the choice of how and where they set up their PNR system, and to decide themselves on the technical aspects of it. The harmonisation aspects are limited to those strictly necessary, such as the technical aspects of the communication systems needed to exchange the data with other Member States.

The financial and administrative burden falling on the community has been minimised through the choice for a decentralised system. Setting up and maintaining a centralised EU system for the collection and processing would entail significant costs.

- **Choice of instruments**

Proposed instruments: Framework Decision based on Article 34(2)(b) TEU.

Other means would not be adequate for the following reason.

As the aim is approximating Member States' legislation, other instruments than a Framework Decision are not appropriate.

4. BUDGETARY IMPLICATION

The proposal has no implication for the Community budget.

5. ADDITIONAL INFORMATION

- **Simulation, pilot phase and transitory period**

There was or there will be a transitory period for the proposal.

- **Review/revision/sunset clause**

The proposal includes a review clause.

2007/0237 (CNS)

Proposal for a

COUNCIL FRAMEWORK DECISION

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

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29, Article 30(1)(b) and Article 34(2)(b) thereof,

Having regard to the proposal from the Commission[2],

Having regard to the opinion of the European Parliament[3],

Whereas,

(1) The European Council adopted the Declaration on combating terrorism on 25 March 2004[4] inviting the Commission to bring forward, inter alia a proposal for a common EU approach to the use of passengers data for law enforcement purposes.

(2) The Commission has been further called upon to bring forward a proposal for the use of PNR in the Hague Programme[5] and at the extraordinary Council meeting of 13 July 2005[6].

(3) It is one of the objectives of the European Union to offer a high level of security and protection within an area of freedom, security and justice; this requires that the prevention of and fight against terrorist offences and organised crime, be carried out in an adequate manner. The definitions of terrorist offences and organised crime are taken from Articles 1 to 4 of the Council Framework Decision 2002/475/JHA on combating terrorism[7] and Article 2 of the Council Framework Decision (xx/xx) on the fight against organised crime[8] respectively.

(4) The Council adopted Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data[9] which aims at improving border controls and

---

2 OJ
3 OJ
4 Bulletin of the EU 3-2004.
5 The Hague Programme – Strengthening Freedom, Security and Justice in the European Union, paragraph 2.2 Terrorism.
6 Council Declaration on the EU response to the London bombings – point 6.
7 OJ L 164, 22.6.2002, p. 3.
8 OJ
9 OJ L 261, 6.8.2004, p. 24.

combating illegal immigration by the transmission of advance passenger data by air carriers to the competent national authorities.

(5) Because of the information they contain, PNR data are appropriate to effectively prevent and fight terrorist offences and organised crime and thus to enhance internal security; the obligations imposed on air carriers by virtue of this Framework Decision should be separate from those established by Directive 2004/82/EC.

(6) Air carriers already collect PNR data for their own commercial purpose and this Framework Decision does not impose any obligation on them to collect any additional information or to retain any data.

(7) To prevent and fight terrorist offences and organised crime, it is essential that all Member States introduce provisions laying down obligations on air carriers operating flights to or from the territory of one or more Member States of the European Union; intra-EU flights should not be covered by this Framework Decision, except those segments connecting two EU-airports which are part of an international flight.

(8) The availability of PNR data to competent national authorities in accordance with the provisions of this Framework Decision is necessary for the purposes of preventing and fighting terrorist offences and organised crime, the regulation of such availability should be proportionate to the legitimate security goal pursued.

(9) The retention period of PNR data by competent national authorities should be proportionate to the purposes for which they are sought; namely the prevention of and fight against terrorist offences and organised crime. Because of the nature of the data and their uses, it is important that the data are kept for a sufficiently long period as to fulfil the purpose of developing risk indicators and establishing patterns of travel and behaviour. In order to avoid a disproportionate use, it is important that after some years, the data is moved to a dormant database and only accessible under very strict and more limited conditions. At the same time this ensures that they are available if they are needed in specified exceptional circumstances. It is also important to permit the extension of the period of retention of the data where such are used in an ongoing criminal investigation or judicial procedure.

(10) The Council Framework Decision (xx/xx) on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters should be applicable to all the data processed in accordance with this Framework Decision. The rights of the data subjects in relation to such processing, such as the right to information, the right of access, the right of rectification, erasure and blocking, as well as the rights to compensation and judicial remedies should be those provided under that Framework Decision.

(11) To ensure the effectiveness of the obligations on air carriers to make PNR data available, dissuasive, effective and proportionate sanctions, including financial penalties, should be provided for by Member States against those air carriers failing to meet these obligations. The Member States should take all necessary measures to enable air carriers to fulfil their obligations under the Framework Decision. In case where there are repeated serious infringementswhich might undermine the basic objectives of this Framework Decision, these sanctions may include measures such as the immobilisation, seizure and confiscation of the means of transport, or the

temporary suspension or withdrawal of the operating licence. Such sanctions should be imposed only in exceptional cases.

(12) It is necessary that competent national authorities are provided with PNR data which are collected by air carriers.

(13) As a result of the legal and technical differences between national provisions concerning information, including PNR, air carriers will be faced with different requirements regarding the types of information to be transmitted, as well as the conditions under which this information needs to be provided to competent national authorities.

(14) These differences may be prejudicial to the effective co-operation between the competent national authorities for the purposes of preventing and fighting.

(15) The Commission in its Communication of 16 December 2003 on 'Transfer of air PNR data: a global EU-approach"[10] has outlined the core elements of an EU policy in this area; it further provided support to and contributed actively to the work undertaken in the framework of the multilateral initiative of ICAO which resulted in the development of the ICAO guidelines on PNR; such guidelines should be taken into account. Measures adopted solely at national or even Union level, without taking into account international coordination and cooperation, would have limited effects. The measures adopted by the Union in this field should therefore be consistent with the work undertaken in international fora.

(16) There are two possible methods of data transfer currently available: the 'pull' method, under which the competent authorities from the State requiring the data can reach into ("access") the air carrier's reservation system and extract ("pull") a copy of the required data and the 'push' method, under which air carriers transmit ("push") the required PNR data to the authority requesting them. The 'push' method is considered to offer a higher degree of data protection and should be mandatory for all carriers established in the Union. As regards third country carriers, "push" should be the preferred method whenever it is technically, economically and operational possible for third country carriers.

(17) PNR data required by a Member State should be transferred to a single representative unit of the requesting Member State.

(18) The contents of any lists of required PNR data to be obtained by the competent national authorities should reflect an appropriate balance between the legitimate requirements of public authorities to prevent and fight terrorist offences and organised crime, thereby improving the internal security within the EU and the protection of fundamental rights of citizens, notably privacy; such list should not contain any personal data that could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life of the individual concerned; the PNR data contain details on the passenger's reservation and travel itinerary which enable competent authorities to identify air passengers representing a risk for internal security.

---

[10] COM(2003) 826, 16.12.2003.

(19) In order to enhance the internal security of the European Union as a whole, each Member State should be responsible for assessing the potential threats related to terrorist offences and organised crime. Guidance for common general criteria for such risk assessment should be provided for by the Committee established by this Framework Decision.

(20) As a fundamental principle of data protection, it is important to ensure that no enforcement action shall be taken by the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation.

(21) Member States should share with other Member States the PNR data that they receive as necessary.. Transfers of PNR data to third countries and adequacy findings should be governed by the Council Framework Decision (xx/xx) on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters and should be further subject to additional requirements relating to the purpose of the transfer, Whenever the Union has concluded international agreements on such transfers, the provisions of such agreements should be duly taken into account.

(22) Member States should ensure that the transfer of the relevant PNR data from air carriers to the competent national authorities takes place using state of the art technological means to guarantee, to the maximum extent possible, the security of the data transmitted.

(23) Since the objectives of this Framework Decision cannot be sufficiently achieved by the Member States acting alone, and can therefore, by reason of the scale and effects of the action, be better achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the EC Treaty and referred to in Article 2 of the EU Treaty. In accordance with the principle of proportionality, as set out in Article 5 of the EC Treaty, this Framework Decision does not go beyond what is necessary to achieve those objectives.

(24) This Framework Decision respects the fundamental rights and observes the principles recognised, in particular by the Charter of Fundamental Rights of the European Union,

HAS ADOPTED THIS FRAMEWORK DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Objectives

This Framework Decision provides for the making available by air carriers of PNR data of passengers of international flights to the competent authorities of the Member States, for the

purpose of preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them.

Article 2

Definitions

For the purpose of this Framework Decision the following definitions shall apply:

(a) ‘air carrier’ means an undertaking with a valid operating licence or equivalent;

(b) "international flight" means any flight scheduled to enter the territory of at least one Member State of the European Union originating in a third country or to depart from the territory of at least one Member State of the European Union with a final destination in a third country;

(c) ‘Passenger Name Record (PNR)’ means a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person. In the context of this Framework Decision, PNR data shall mean the data elements described in the Annex and only to the extent that these are collected by the air carriers;

(d) 'passenger' means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the carrier;

(e) ‘reservation systems’ means the air carrier’s internal inventory system, in which PNR data are collected from reservations made via computerised reservation systems as defined in Regulation (EEC) No 2299/89 on a code of conduct for computerized reservation systems or via direct booking channels like the airlines’ Internet websites, call centres or sales outlets;

(f) 'Push method’ means the method under which air carriers transmit the required PNR data into the database of the authority requesting them;

(g) "Pull method" means the method under which the authority requiring the data can access the air carrier's reservation system and extract a copy of the required data into their database;

(h) "terrorist offences" means the offences under national law, referred to in Articles 1 to 4 of the Council Framework Decision 2002/475/JHA on combating terrorism[11];

(i) "organised crime" means the offences under national law, referred to in Article 2 of the Council Framework Decision (xx/xx) on the fight against organised crime[12].

---

11 OJ L 164, 22.6.2002, p. 3.

12 OJ

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 3

Passenger Information Unit

1. Within twelve months after this Framework Decision enters into force, each Member State shall designate a competent authority, hereafter called "Passenger Information Unit", and notify it to the Commission and the General Secretariat of the Council, and may at any time update its declaration. The Commission shall publish this information in the *Official Journal of the European Union.*

2. The Passenger Information Unit shall be responsible for collecting the PNR data from the air carriers or the intermediaries, according to Articles 5 and 6, in relation to international flights which arrive or depart from the territory of the Member States which it serves. To the extent that the PNR data of a passenger as collected, includes data additional to those included in the Annex or special categories of personal data that would reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life of the person concerned, the Passenger Information Unit shall delete such data immediately.

3. The Passenger Information Unit shall further be responsible for analysing the PNR data and for carrying out a risk assessment of the passengers in order to identify the persons requiring further examination for one of the purposes mentioned in paragraph 5. The criteria and guarantees in respect of this risk assessment will be provided for under national law. No enforcement action shall be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation.

4. The Passenger Information Unit of a Member State shall transmit the PNR data of individuals identified in accordance with paragraph 3 to the relevant competent authorities of the same Member State, referred to in Article 4, by electronic means or, in case of failure, by any other appropriate means.

5. The PNR data of passengers may only be processed by the Passenger Information Units and the competent authorities of the Member States, referred to in Article 4, to prevent or combat terrorist offences and organised crime, for the following purposes:

   – to identify persons who are or may be involved in a terrorist or organised crime offence, as well as their associates;

   – to create and update risk indicators for the assessment of such persons;

– to provide intelligence on travel patterns and other trends relating to terrorist offences and organised crime;

– to be used in criminal investigations and prosecutions of terrorist offences and organised crime.

The Passenger Information Units and the competent authorities shall not take any enforcement action solely on the basis of the automated processing of PNR data.

6. Two or more Member States may establish or designate the same authority to serve as their Passenger Information Unit. Such Passenger Information Units shall be considered the national Passenger Information Unit of all such participating Member States.

Article 4

Competent authorities

1. Each Member State shall adopt a list of the competent authorities which shall be entitled to receive PNR data from the Passenger Information Units and to process them.

2. Competent authorities shall only include authorities responsible for the prevention or combating of terrorist offences and organised crime.

3. Each Member State shall notify the list of its "competent authorities" in a declaration to the Commission and the General Secretariat of the Council within twelve months after this Framework Decision enters into force, and may at any time update its declaration. The Commission shall publish the declarations in the *Official Journal of the European Union*.

Article 5

Obligation on air carriers

1. Member States shall adopt the necessary measures to ensure that air carriers make available the PNR data of the passengers of international flights to the national Passenger Information Unit of the Member State on whose territory the international flight referred to is entering, departing or transiting, in accordance with the conditions specified in this Framework Decision.

2. Air carriers shall make available to the Passenger Information Unit the PNR data specified in the Annex to the extent that they are collected and processed in the air carriers' reservation systems.

3. Air carriers shall make available such data by electronic means or, in case of failure, by any other appropriate means:

(a) in advance, 24 hours before the scheduled flight departure

and

(b) immediately after flight closure.

The relevant Passenger Information Unit may require an air carrier to make available to it PNR data prior to 24 hours before the scheduled flight departure, when there is an indication that early access is necessary to assist in responding to a specific threat related to terrorist offences and organised crime. In exercising this discretion, the Passenger Information Unit will act proportionally.

4. Air carriers whose databases are established in a Member State of the European Union shall take the necessary technical measures to ensure that the PNR data are transferred to the Passenger Information Units or the designated intermediaries pursuant to Article 6, using the "push method".

5. Air carriers whose databases are not established in a Member State of the European Union:

– shall be required to use the "push method" to transfer the data to the Passenger Information Units or the designated intermediaries pursuant to Article 6;

– where they do not possess the necessary technical architecture to use the "push method", shall be obliged to permit the Passenger Information Unit or the designated intermediary pursuant to Article 6, to extract the data from their databases using the "pull method".

In all cases, they must inform the Passenger Information Units and the relevant intermediaries of all the Member States whether they will use the "push" or the "pull" methods for making the data available.

6. Member States shall ensure that air carriers inform passengers of international flights about the provision of PNR data to the Passenger Information Unit and, where applicable, the intermediary, the purposes of their processing, the period of data retention and their possible use to prevent or combat terrorist offences and organised crime, and about the possibility of exchanging and sharing of such data.

Article 6

Intermediary

1. Members States shall ensure that air carriers that operate international flights may designate an intermediary to which they make the PNR data of passengers available, instead of making such data available directly to Passenger Information Units, subject to paragraphs 2 to 6.

2. Air carriers entering into contractual relationships with such intermediaries shall notify immediately the Passenger Information Units of all Member States of such an arrangement. The intermediaries shall act on behalf of the air carrier from which they have been designated, and they shall be considered as such air carrier's representative for the purposes of this Framework Decision.

3. Intermediaries designated by air carriers shall be responsible for collecting the PNR data from the air carriers. To the extent that the PNR of a passenger as collected, includes data additional to those referred to in the Annex or special categories of personal data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life of the person concerned, the intermediary shall immediately delete such data.

4. Intermediaries shall further transmit the PNR data to the national Passenger Information Unit of the Member State on whose territory the international flight referred to is entering, departing or transiting, by electronic means or, in case of failure, by any other appropriate means. The transmission of such data to the Passenger Information Unit shall be done by using the "push" method.

5. Intermediaries shall keep their databases and carry out the processing of PNR only in the territory of the European Union.

6. Intermediaries shall be prohibited from processing the data collected from the air carriers and transmitted to the Passenger Information Unit for any purpose, other than those mentioned in this Article; they shall delete the data immediately after transmission to the relevant Passenger Information Unit.

Article 7

Exchange of Information

1. Member States shall ensure that the PNR data of persons identified by a Passenger Information Unit in accordance with Article 3(3) shall be transmitted by that Passenger Information Unit to the Passenger Information Units of other Member States only in such cases and to the extent that such transmission is necessary in the prevention and fight against terrorist offences and organised crime. The Passenger Information Units of the receiving Member States shall retain the PNR data in accordance with Article 9 and transmit them to their relevant competent authorities designated pursuant to Article 4.

2. The Passenger Information Unit or any of the designated competent authorities of a Member State shall have the right to request the Passenger Information Unit of any other Member State to provide it with specific PNR data which are kept in the latter's active database as per Article 9(1). The request for such data may be based on any one or a combination of data elements, as deemed appropriate by the requesting Unit for the prevention or combat of terrorist offences and organised crime. Passenger Information Units shall respond to such requests as soon as they are able to extract such data.

3. When a Member State requests specific PNR data of another Member State which are kept in the dormant database as per Article 9(2), the request shall be made to the authority which is responsible in the Member State for the database containing the PNR data, and shall be made only in exceptional circumstances in response to a specific and actual threat related to the prevention or combat of terrorist offences and organised crime. Access to such data shall be limited to personnel of the competent authorities which will be specifically authorised for this purpose.

4. In exceptional circumstances, when there is an indication that early access is necessary to assist in responding to a specific and actual threat related to the prevention or combat of terrorist offences and organised crime, the Passenger Information Unit of a Member State or the designated competent authorities shall have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights arriving or, departing from the latter's territory prior to 24 hours before the scheduled flight departure.

Article 8

Tranfer of Data to Third Countries

1. In addition to the conditions and safeguards contained in the Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters, PNR data may be provided by a Member State to law enforcement authorities of third countries only if the Member State is satisfied that:

   (a) the authorities of the third country shall only use the data for the purpose of preventing and fighting terrorist offences and organised crime,

   (b) such third country shall not transfer the data to another third country without the express consent of the Member State.

2. In addition, such transmissions may only take place in accordance with the national law of the Member State concerned and any applicable international agreements.

Article 9

Period of data retention

1. Member States shall ensure that the PNR data provided by the air carriers or the intermediaries to the Passenger Information Unit are kept in a database at the Passenger Information Unit for a period of five years after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is entering, departing or transiting.

2. Upon the expiry of the period of five years of the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be kept for a further period of eight years. During this period, the PNR data may be accessed, processed and used only with the approval of the competent authority and only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime. Access to such data shall be limited to personnel of the competent authorities which will be specifically authorised for this purpose.

3. Member States shall ensure that the PNR data are deleted from the databases of their Passenger Information Unit upon the expiry of the period of eight years specified in paragraph 2.

4. By way of derogation from paragraphs 1, 2 and 3, the Passenger Information Units shall be allowed to retain the PNR data for longer periods in cases where the data is being used for an ongoing criminal investigation of a terrorist offence or an organised crime against or involving the data subject. Such data shall be deleted from all records and files once such an investigation is concluded.

Article 10

Sanctions

Member States shall ensure, in conformity with their national law, that dissuasive effective and proportionate sanctions, including financial penalties, are provided for against air carriers and intermediaries which do not transmit data or transmit incomplete or erroneous data or otherwise infringe the national provisions adopted pursuant to this Framework Decision. In case of repeated serious infringements, these sanctions shall include measures such as the immobilisation, seizure and confiscation of the means of transport, or the temporary suspension or withdrawal of the operating licence.

CHAPTER III

PROTECTION OF PERSONAL DATA

Article 11

Protection of personal data

1. Member States shall ensure that the Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (xx/xx)[13] is applicable to the processing of personal data under this Framework Decision.

2. Data which is received pursuant to this Framework Decision by the Passenger Information Units, the intermediaries and the designated competent authorities of all the Member States shall exclusively be processed for the purposes of the prevention, detection, investigation and prosecution of terrorist offences or organised crime.

3. No enforcement action shall be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation.

---

13 OJ

Article 12

Data security

Member States shall ensure that the Passenger Information Units, the intermediaries and the competent authorities of each Member State shall adopt the necessary security measures with respect to PNR data which is processed pursuant to this Framework Decision in order to:

a) physically protect data;

b) deny unauthorised persons access to national installations in which the Member State store data (checks at entrance to the installation);

c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

d) prevent the unauthorised inspection, modification or deletion of stored personal data (storage control);

e) prevent the unauthorised processing of data (control of data processing);

f) ensure that persons authorised to access the data have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);

g) ensure that all competent authorities with a right to access the data create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities without delay upon their request (personnel profiles);

h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);

i) prevent the unauthorised reading and copying of personal data during their transmission, in particular by means of appropriate common protocols and encryption standards (transport control).

CHAPTER IV

COMITOLOGY

Article 13

Common Protocols and Encryption standards

1. Until the time limit referred to in paragraph 6 of this Article has elapsed, all transmissions of PNR data made for the purposes of this Framework Decision shall be made by electronic means or, in case of failure, by any other appropriate means.

2. Once the time limit referred to in paragraph 6 of this Article has elapsed, all transmissions of PNR data made for the purposes of this Framework Decision shall be made electronically using secure methods common to all transmissions to ensure the security of the data during transmission and their readability by all parties involved, which shall include the following:

   a) common protocols, and

   b) common encryption standards.

3. The common protocols and encryption standards shall be set up and, if need be, adapted in accordance with the procedure provided for in Article 15.

4. If the mode of transmission referred to in paragraphs 2 and 3 is not available, paragraph 1 shall remain applicable for the entire period of such unavailability.

5. Each Member State shall ensure that the necessary technical alterations are carried out to be able to use the common protocols and encryption standards for all transmissions of PNR data made for the purposes of this Framework Decision. Member States shall notify the Commission of the date from which such transmissions can be carried out. The Commission shall immediately inform the Committee referred to in Article 14.

6. The technical alterations referred to in paragraph 5 shall be carried out within 1 year from the date the common protocols and the encryption standards are adopted.

7. The measures necessary for the implementation of paragraphs 2 and 3 shall be adopted in accordance with the regulatory procedure referred to in Article 15.

Article 14

Committee procedure

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission (the "Committee").

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the *Official Journal of the European Union*.

3. It may give appropriate recommendations to its members on the adoption of common protocols and encryption standards which shall be used in all PNR transmissions under this Framework Decision as well as the common general criteria, methods and practices for the risk assessment according to Article 3(3).

Article 15

Procedure

1. Where reference is made to this Article, the representative of the Commission shall submit to the Committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the Chair may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty establishing the European Community, in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the Committee shall be weighted in the manner set out in that Article. The Chair shall not vote.

2. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee.

3. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall without delay submit to the Council a proposal on the measures to be taken and shall inform the European Parliament thereof.

4. The Council may act by qualified majority on the proposal, within three months from the date of referral to the Council.

   If within that period the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, re-submit its proposal or present a legislative proposal on the basis of the Treaty.

   If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

CHAPTER V

FINAL PROVISIONS

Article 16

Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision before 31 December 2010. By the same date they shall transmit to the General Secretariat of the Council and the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision and a correlation table between those provisions and this Framework Decision.

When Member States adopt those provisions, they shall contain a reference to this Framework Decision or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. On the basis of a report established using this information and a written report from the Commission, the Council shall before 31 December 2011 assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 17

Review

On the basis of information provided by the Member States, the Commission shall undertake a review of the operation of this Framework Decision and shall submit a report to the Council within three years after this Framework Decision enters into force. Such review shall comprise all the elements of this Framework Decision, with special attention of the implementation of the "push method", the level of adherence to the data protection safeguards, the evaluation of the length of the data retention period and the quality of the risk assessments.

Article 18

Statistical data

1. Member States shall ensure that a set of statistical information on PNR data provided to the Passenger Information Units is available.

2. Such statistics should as a minimum cover per air carrier and destination the number of information elements, the number of identifications of high risk persons and the number of subsequent law enforcement actions involving the use of PNR data.

3. These statistics should not contain any personal information. They should be transmitted to the General Secretariat of the Council and the Commission on a yearly basis.

Article 19

Relation to other instruments

1. Member States may continue to apply bilateral or multilateral agreements or arrangements in force when this Framework Decision is adopted in so far as such agreements or arrangements are compatible with the objectives of this Framework Decision.

2. Member States may conclude or bring into force bilateral or multilateral agreements or arrangements after this Framework Decision has come into force in so far as such

agreements or arrangements are compatible with the objectives of this Framework Decision.

Article 20

Entry into force

This Framework decision shall enter into force the day following its publication in the *Official Journal of the European Union*.

Done at Brussels,

For the Council
The President

ANNEX

PNR data pursuant to Article 2

Data for all passengers

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name (s)

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

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

(7) All travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency /Travel agent

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

(11) Split/Divided PNR information

(12) General remarks (excluding sensitive information)

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

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any collected API information

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

Additional data for unaccompanied minors under 18 years

(1) Name and gender of child

(2) Age

(3) Language(s) spoken

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

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

(6) Departure and arrival agent