COUNCIL OF THE EUROPEAN UNION

Brussels, 17 April 2008

7656/2/08 REV 2

Interinstitutional File: 2007/0237 (CNS)

CRIMORG 49
AVIATION 77
DATAPROTECT 14

NOTE

from :	Presidency
to :	Multidisciplinary group on organised crime
prev doc no: :	14922/07 CRIMORG 169AVIATION 193 DATAPROTECT 49 6325/08 CRIMORG 30 AVIATION 39 DATAPROTECT 6 + COR + COR 2
Subject :	Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes

1. Introduction

The Commission submitted the above proposal for a framework decision to the Council on 17 November 2007 and briefly presented its contents to the Multidisciplinary group on organised crime (MDG) on 30 November 2007. At the Informal JHA Ministerial meeting on 25-26 January 2008, the Ministers of Interior discussed a number of general questions regarding this Commission proposal. It resulted from the discussions that there was very broad support for the idea of setting up a European system of using PNR data for law enforcement purposes.

Articles 1 through 12 of the above Commission proposal were discussed at meetings of the Multidisciplinary group of 4 February, 25 and 26 March and 15 April 2008 and at the meeting of the Friends of the Presidency of 25 February 2008.

AT entered a reservation on the proposal. The following delegations entered a general scrutiny reservation on the proposal: BE, BG, CZ, DK, FI, HU, IT, LU, LV, LT, MT, PL and SK. In addition, a number of delegations also entered a parliamentary scrutiny reservation: AT, CZ, DK, EE, FR, HU, IE, LT, MT, NL, PL, PT, SE and UK. DE welcomed that the Commission had tabled a proposal on the use of PNR data, as requested by the Council. DE however pointed out that specific provisions of the Draft Framework decision still needed a thorough examination in order to ensure that it would be compatible with all data protection and constitutional requirements.

The Presidency has redrafted Articles 1-12 in order to accommodate as much as possible as possible the comments made by delegations. Consultations with the air carrier industry are also on-going and may provide further input for future discussions of these articles. Once the discussion of Articles 13 and following will have been finalised, the Presidency deems it appropriate to discuss again a number of general questions before commencing the second reading. These questions are set out hereafter.

2. Limitation of scope:

The Commission proposal's scope is limited in several respects. At the MDG meeting of 4 February 2008, the Presidency asked for delegations' positions with regard to these limitations and in particular whether they considered these limitations should be both the minimum and the maximum standard (i.e. Member States may not go beyond them in their domestic law) or minimum standards only, which would allow them to give a wider scope to their domestic legislation than will be required under EU law.

Regarding the modes of transport (air carriers only) and the geographical scope (no purely intra-EU flights), the Presidency thinks it is better not to reopen this discussion at this stage, even though it is aware that a number of delegations[1] continue to have reservation on the latter limitation.

[1] DK (supported by EE) thought intra EU flights should be included as well and therefore entered a scrutiny reservation on the exclusion of the flights from the scope of the Commission proposal BE, FR and GR. IT and SE also stressed that screening of intra EU flights could be useful for law enforcement purposes in some cases.

The most important limitation is undoubtedly that of the scope of the proposal to the fight against terrorism and organised crime. At least two important questions should be resolved in this respect. First, several Member States criticised the reference to organised crime for being too narrow and indicated that forms of serious crime should be included in the scope of the proposal instead of only terrorism and participation in organised crime. The Presidency proposes to base the discussion on the scope of purpose limitation on the definition of serious crime within the meaning of Article 4(1) of the draft Council Decision establishing the European Police Office (EUROPOL). This provision refers to forms of serious crime listed in the Annex to that draft decision, which in turn has the same list of offences as in Article 2 of the Framework Decision on the European arrest warrant.
Second, most delegations have expressed themselves to be in favour of an *intermediate option*, whereby the purpose limitation laid down in the draft Framework decision would be binding as to processing of PNR data (most notably risk assessment). However, should the follow-up action by the competent authorities ultimately reveal indications of other criminal offences, the purpose limitation would not interfere with national powers to investigate and prosecute such offences. The Presidency invites delegations to consider whether the redraft of Articles 3(3) and 4(4)(5) embodies this idea in a sufficiently clear manner.
Third, delegations are invited to express themselves with regard to the question whether Member States should be allowed to go beyond the purpose limitation of the EU text under their domestic law, as a few delegations have previously argued[1].

3. Possible impact of the PNR proposal on relations with third countries

Article 8 of the draft proposal allows the transfer of PNR data and analytical information flowing from PNR data to third countries under certain conditions. However, the setting up of PNR systems in the Member States will, in certain cases, necessitate data flows from third countries to the Member States, as the relevant PNR data may be located in third countries. This prompts the question whether PNR agreements would need to be negotiated with third countries in order to allow these data flows. Whether a PNR agreement is required for obtaining PNR data from a third country will be determined by the third countries in question. Hence it is not possible to answer this question in a general manner.

[1] CY, FR and UK previously indicated that Member States should be able to do so.

In addition, third countries may request reciprocity for the provision of PNR data to the EU, by requesting that EU-sourced PNR data be transferred to them, which might require the EU to negotiate PNR agreements with these countries. The Commission proposal does not provide anything on such PNR agreements with third countries, but several delegations have made it clear that the impact of this proposal on the relations with third countries should be carefully taken into account.

Hence the Presidency invites delegations to consider whether:

1) the PNR Framework decision should provide certain standards for such PNR agreements with third countries;

2) if so, which should be these standards.

4. Data protection

Regarding the data protection rules for the protection of the data subject, Directive 95/46 will apply as long as these data are processed by the air carriers for commercial purposes. No new rules need to be devised in that respect.

However, the transmission of those data from air carriers to the PIU may not be covered by the Directive, nor by the DPFD. Therefore, the Presidency deems that, contrary to the initial Commission proposal, data protection rules need to be provided as from the stage of the transmission of the PNR data by the air carriers to the PIUs. Irrespective of the questions with regard to the exact legal base of any future provisions to that end (which should be addressed at a later stage), this issue should also be regulated and the Presidency has therefore proposed specific data protection rules, relying on the solutions in the DPFD proposal.

Once the PNR data are transmitted to the PIUs, Article 11 of the original Commission proposal provided that rules of the DPFD should apply. A few delegations pointed out that the formal scope of the DPFD was limited to cross-border exchange of personal data only. Others thought that more clarity and protection could be gained by setting out, in the PNR Framework decision itself, which specific data protection rules applied. The Presidency has endeavoured to do so, but at the MDG meeting of 15 April 2008, a few delegations argued in favour of so-called constituent reference to the DPFD rules, by which the DPFD rules would be made applicable. The Presidency concurs with those delegations which think that this is impracticable as it will often not be clear which data protection rules apply and the DPFD rules are too general in this regard.

The Presidency invites delegations to decide whether they want:

1) specific data protection rules in the PNR instrument; or

2) a constituent reference to the DPFD rules.

In case, the choice is made for the first option, the Presidency invites delegations to indicate whether they think the data protection rules in the PNR instrument should be confined to PNR data held by PIUs or should also encompass the processing of PNR data by competent authorities.

The Presidency has opted to limit the data protection provisions to PNR data held by the PIUs for the reasons set out hereafter. The Presidency proposes recitals 10a and 10b as a reminder of the applicability of data protection rules in the DPFD or in matching national data protection rules, to PNR data held by competent authorities or to PNR data exchanged cross-border.

As indicated, the Presidency has started from the basic assumption that this Framework decision should lay down data protection provisions only with regard the PNR data processed by PIUs when receiving and analysing these data (apart from the transmission by air carriers).

On the contrary, the Presidency does not think that it is necessary, nor expedient to lay down data protection provisions for the handling of (the analysis of) PNR data by the competent (law enforcement) authorities. At least three arguments militate against setting up a specific data protection framework for handling of PNR data by law enforcement authorities. First, the Council has reached a general approach on the DPFD in November 2007, by virtue of which Member States will provide for the data protection safeguards to handling of personal data, including PNR data, by law enforcement authorities. This will follow either from the DPFD directly or from the obligation to provide for matching national data protection standards (recital 6a of the DPFD). Second, it is difficult to see why the data protection provisions applicable to the handling of PNR data by law enforcement authorities should be different according to whether the PNR data have been obtained through a PIU or by a law enforcement agent at the border who asks, on an ad hoc basis, for a passenger's PNR data. Third, it would seem that there is a risk of confusion in setting up a specific data protection regime different from the general data protection regime for law enforcement authorities.

As to the specific situation in which competent authorities would receive and process bulks of raw PNR data, the Presidency is of the opinion that, should such possibility be accepted, the competent authority should then also abide by the data protection rules of this Framework decision as it is in effect exercising the role of a PIU.

5. Use of sensitive data

The Commission proposal absolutely excludes the processing of sensitive data, by stating in Article 6(3) that, to the extent that the PNR of a passenger includes such data, the intermediary shall immediately delete such data. At the meetings of 4 and 25 February 2008, the Presidency asked for delegations' positions with regard to this exclusion. A group of several Member States advocated in favour of the possibility to use such data in exceptional circumstances, whereas a comparable group of Member States supported the approach in the Commission proposal.

The presentations of various existing PNR systems in the framework of the Friends of the presidency meeting of 27 March 2008 also related to the use of sensitive data and the accompanying safeguards for such use. Against this background, the Presidency invites delegations to clarify their positions as follow:

1) could sensitive PNR data be used under exceptional circumstances to prevent actual threats to public security or vital interests of the data subjects, provided that such use would be restricted to individual passenger's PNR data and could never be used for automated processing of PNR data (most notably, risk assessments);

2) in affirmative, which safeguards would be needed to govern the use of such data.

6. Data retention period

The Presidency has invited delegations to come back with actual proposals about the optimum period for data retention.

The Presidency invites the Member States:

(i) to present such proposals

(ii) to clarify whether they would like to keep the distinction between active and inactive databases.

ANNEX

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[3],

Having regard to the opinion of the European Parliament[4],

Whereas,

(1) The European Council adopted the Declaration on combating terrorism on 25 March 2004[5] 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[6] and at the extraordinary Council meeting of 13 July 2005[7].

---

3 OJ

4 OJ

5 7906/04.

6 The Hague Programme – Strengthening Freedom, Security and Justice in the European Union, paragraph 2.2 Terrorism.

7 Council Declaration on the EU response to the London bombings – point 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, detection, investigation and prosecution of 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[8] and Article 2 of the Council Framework Decision (xx/xx) on the fight against organised crime[9] respectively.

(4) The Council adopted Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data[10] which aims at improving border controls and 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, detect, investigate and prosecute[11] 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 from their passengers for their own commercial purposes. This Framework Decision does not impose any obligation on air carriers to collect any additional information from passengers or to retain any data or any obligation on passengers to provide any data in addition to that already provided to air carriers on a voluntary basis.

---

8 OJ L 164, 22.6.2002, p. 3.

9 OJ

10 OJ L 261, 6.8.2004, p. 24.

11 Throughout the text, the term 'fight' has been replaced by the terms ' detect, investigate and prosecute'.

(7) To prevent, detect, investigate and prosecute 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, detecting, investigating and prosecuting 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, detection, investigation and prosecution of 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) (...) Data protection rules applicable to all PNR data processed by the Passenger Information Units and air carriers in accordance with this Framework Decision should be clear and unambiguous and 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 (...), as well as the rights to compensation and judicial remedies should be those provided under this Framework Decision.

(10a) The transfer of PNR data , by the Passenger Information Unit[12] of one Member State to the Passenger Information Unit or the competent authority of another Member State is subject to the data protection safeguards laid down in 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), as is the exchange of PNR data between the competent authorities of various Member States[13].

(10b) The processing of PNR data , by competent authorities is equally subject to the data protection safeguards laid down in 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) or to national data protection rules which match those data protection safeguards. However, it is necessary to derogate from the latter Framework decision by imposing more stringent the rules regarding the possible use of PNR data in this 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 infringements which 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 BE thought PIUs were not necessarily law enforcement authorities and that the DPFD would therefore not necessarily be applicable. The Presidency would like to point out that regardless of the status of PIUs under domestic law, their function will de facto always be one of assistance in the detection and investigation of possible criminal offences. Hence the DPFD would always be applicable in the situation described in recital 10a.

13 CZ and PL suggested to put this into the body of the text. The Presidency would like to indicate that this recital is merely declaratory. As a reminder of the applicability of the DPFD, it therefore is not required to be put into the text.

(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, detecting, investigating and prosecuting and fighting terrorist offences and organised crime.

(15) The Commission in its Communication of 16 December 2003 on 'Transfer of air PNR data: a global EU-approach"[14] 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.

---

[14] COM(2003) 826, 16.12.2003.

(17) PNR data required by a Member State should be transferred to a single representative unit (Passenger Information Unit) of the requesting Member State, as to ensure clarity and reduce the costs to air carriers.

(17a) Air carriers that operate international flights may designate an intermediary through which they make the PNR data of passengers available, instead of making such data available directly to Passenger Information Units. Where such intermediaries are designated, they 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. The designation of such intermediary does not exonerate the air carrier from its obligations under this Framework Decision.

(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, detect, investigate and prosecute 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.

(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 decision which produces an adverse legal effect to a person or seriously affects him 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.

(21a) The Framework Decision rules on exchange of PNR data between the Passenger Information Units of different Member States are without prejudice to the exchange of PNR data between law enforcement or judicial authorities that have obtained PNR data from their Passenger Information Unit in accordance with this Framework Decision. Such exchange of PNR data between law enforcement or judicial authorities shall be governed by the rules on international police and judicial co-operation.

(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 detecting, investigating and prosecuting terrorist offences and organised crime, as well as the processing of those data, including their collection, use and retention (...) by these authorities and their exchange (...) between them.

Article 2

Definitions [15]

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

(a) 'air carrier' means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage by air of passengers, as stated in the operating licence;

(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[16];

[15] SE scrutiny reservation.

[16] Two Member States (DK, EE) pleaded in favour of the inclusion of intra-EU flights.

(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. Such a record may be contained in reservation systems, Departure Control Systems (DCS), Global Distribution Systems (GDS) or equivalent systems, or is otherwise known by the air carrier[17]. 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 or otherwise known by the air carriers;

(d) 'passenger' means any person, except members of the crew[18], carried or to be carried in an aircraft with the consent of the carrier;

(e) 'reservation systems' means the air carrier's computerised 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 air carriers' 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, departure control system, Global Distribution System and equivalent system and extract (...) the required data into their database;

(h) "terrorist offences" means the offences under national law, referred to in Articles 1 to 4[19] of the Council Framework Decision 2002/475/JHA on combating terrorism;

(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[20].

---

17 Suggested clarification of the type of data covered by the Framework Decision.

18 UK wanted to include crew members.

19 BE thought it was sufficient to mention Article 2 and it was not necessary to include Articles 1, 3 and 4.

20 Several Member States (BE, CY, CZ, EE, ES, HU, SE and UK) criticised this reference to organised crime for being too narrow and indicated that forms of serious crime should be included in the scope of the proposal instead of the only membership of a

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 3

Passenger Information Unit[21]

1. (....) Each Member State shall set up or designate a public authority, to act as its "Passenger Information Unit". The Passenger Information Unit may be designated from authorities of the Member State which are responsible for the prevention, detection, investigation or prosecution of terrorist offences and organised crime. It may also be a separate branch of a competent authority as defined in Article 4[22]. Each Member State shall notify its Passenger Information Unit 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 notification. The Commission shall publish this information in the *Official Journal of the European Union.*

---

criminal organisation. In this perspective, inspiration might be drawn from the draft Council Decision establishing the European Police Office (EUROPOL), which in Article 4(1) refers to forms of serious crime listed in the Annex to that draft decision. That Annex in turn has the same list of offences as in Article 2 of the Framework Decision on the European arrest warrant.

[21] CZ and DE scrutiny reservation.

[22] Several delegations (EE, LU, FR, SE) asked that the Framework Decision would allow the PIU to be a branch of the law enforcement authority competent for acting upon the PNR.

2. The Passenger Information Unit shall be responsible for collecting the PNR data from the air carriers (...), according to Article 5 (...), 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 upon their receipt[23].

3. The Passenger Information Unit shall further be responsible for analysing the PNR data and for carrying out a risk assessment of the [24] passengers in order to identify the persons requiring further examination by the competent authorities of the Member State, as referred to in Article 4[25]. Such analysis and risk assessment shall be aimed at preventing, detecting, investigating or prosecuting terrorist offences and organised crime, only 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[26].

---

[23] CZ and PT scrutiny reservation on paragraph 2. CY, DE, EE, IT, SE and UK scrutiny reservation on the need for a general obligation to delete all sensitive data. BE, ES, GR and HU were in favour of such general obligation. MT thought this should be left to the PIU.

[24] DE indicated that it thought Member States should not be under an obligation to analyse the PNR data of all passengers.

[25] Some delegations pleaded in favour of some degree of harmonisation with regard to the risk assessment: AT, LU, PT, SK.

[26] AT, DE, IE and HU scrutiny reservation.

The criteria and guarantees in respect of such risk assessments will be provided for under national law, which shall take due account of the recommendations for common general criteria, methods and practices for the risk assessment adopted under the procedure of Articles 13, 14 and 15. No risk assessment criterion shall be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation.

4. The Passenger Information Unit of a Member State shall transmit the analytical information flowing from PNR data of individuals identified in accordance with paragraph 3 for potential further examination 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[27]. The Passenger Information Units shall not take any decision on the basis of a passenger's PNR data which produces an adverse legal effect concerning a person or significantly affects him.

5. (...)

6. Two or more Member States may jointly set up or designate the same authority to serve as their Passenger Information Unit. Such Passenger Information Units shall be established in one of the participating Member States and shall be considered the national Passenger Information Unit of all such participating Member States[28]. The participating Member States shall agree on the modalities of the operation of the Passenger Information Unit, the control of the data and in particular on the applicable requirements on data security, data protection and supervision, in accordance with the requirements laid down in this Framework decision.

---

[27] HU indicated telex might be used. SE asked for the deletion of of alternative means. UK scrutiny reservation.

[28] AT and SK pleaded in favour of a supranational analysis of PNR data.

Article 4

Competent authorities

1. Each Member State shall adopt a list of the competent authorities which shall be entitled to receive analytical information flowing from PNR data from the Passenger Information Units in order to examine this information further .

2. Competent authorities shall only include authorities of the Member States which are responsible for the prevention, detection, investigation or prosecution 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*.

4. The PNR data of passengers may be processed by the competent authorities of the Member States only with the aim of preventing, detecting, investigating or prosecuting terrorist offences and organised crime.

5. The limitation set out in paragraph 4 shall not affect or interfere with national law enforcement or judicial powers in case other offences, or indications thereof, are detected in the course of follow-up enforcement action further to such processing.

6. The competent authorities of the Member States shall not take any decision which produces an adverse legal effect on a person or significantly affects him only by reason of an automated processing of PNR data or only on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership or health or sexual orientation.

Article 5

Obligation on air carriers

1. Member States shall adopt the necessary measures[29] 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. In cases in which a transiting international flight includes a segment involving two or more different Member States, air carriers should make available the PNR data of the passengers to the Passenger Information Units of all the involved Member States[30].

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 or otherwise known by the air carrier. For the purposes of this Framework Decision, PNR data shall be deemed to be collected or otherwise known by the air carrier if it is collected and processed in the air carriers' reservation systems, departure control systems, Global Distribution Systems (GDS) and equivalent systems, or is requested in the course of business of the air carrier but not necessarily held in such a system.

---

[29] PL reservation on paragraph 1. PL in particular queried the meaning of 'necessary measures'.

[30] Addition to accommodate a remark made by FR with regard to transit flight in the context of the discussion on Article 2(b). However, the question may need further reflection, in particular, as all the PNR data of a international flight entering the EU will be communicated to the PIU of the Member State concerned, including those of transit passengers.

3. Air carriers shall make available such data by electronic means using the common protocols and encryption standards to be adopted according to the procedure of Articles 13, 14 and 15, or, in case of technical failure, by any other appropriate means[31]:

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

and

(b) immediately after flight closure[32].

In specific cases, when there is an indication that early access is necessary to assist in responding to a specific and actual[33] threat related to terrorist offences and organised crime, a Passenger Information Unit may, in accordance with national law[34], require an air carrier to make available to it PNR data prior to 24 hours before the scheduled flight departure. [In exercising this discretion, the Passenger Information Unit will act proportionally][35].

---

31 Several delegations (FR, HU) questioned the concept of 'appropriate means'. The Presidency has tried to clarify the electronic transmission mode that would as a rule apply. As the 'appropriate means' would be used only in case of a technical failure, it may not be necessary to further specify these 'appropriate means'.

32 Delegations discussed this two-step approach and the criterion of 24 hours. As all delegations agreed on the need to have a harmonised approached, but disagreed on the exact criterion, the Presidency invited delegations to reflect on the most adequate moment for transmitting PNR data. Some delegations asked that the second transmission be limited to those PNR data that have changed after the first transmission. The concept of 'flight closure' also needed to be clarified. EE linguistic reservation on the concept of flight closure.

33 Addition in order to ensure consistency with Article 7(4). MT and UK argued in favour of a lower threshold without need to demonstrate the actual nature of the threat.

34 Following an intervention by DE, the Presidency suggests this addition in order to clarify that the ad hoc powers of PIUs to request PNR data in specific cases are regulated by national law. This sentence merely acknowledges the possibility for national law to provide for such powers, in addition to the general EU obligation to transmit PNR data, set out at the beginning of paragraph 1.

35 PT asked what was meant by 'proportionally'. COM replied by stating that it was meant to emphasise that such requests could only be made on an ad hoc basis. As, the proportionality principle is a general principle of law, the Presidency thinks that this could be left to Member States law and this sentence could maybe be deleted.

4. Air carriers using databases that 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 (...), using the "push method".

5. [Air carriers using databases that 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 (...);

   – where they do not possess the necessary technical architecture to use the "push method", shall be obliged to permit the Passenger Information Unit (...), to extract the data from their databases using the "pull method".

   In all cases, they must inform the Passenger Information Units (...) of all the Member States whether they will use the "push" or the "pull" methods for making the data available[36].]

6. Member States shall ensure that air carriers inform passengers in accordance with Article 11c of this Framework Decision[37].

---

[36] Several delegations (CZ, DE, FR, HU, IT, PL) questioned the subsidiary 'pull' alternative, which is offered to the air carriers with a database outside the EU. It was suggested that this might result in a competitive advantage for air carriers outside the European Union. The Presidency concluded that further reflection was required on the need/expediency to distinguish between EU and non-EU carriers, and on the criterion for such distinction.

[37] At the request of several delegations (BE, ES, MT, PL, PT), the Presidency suggests to move this paragraph to the Data Protection Chapter.

Article 6

Intermediary[38]

(...)

Article 7

Exchange of Information

1. Member States shall ensure that the analytical information flowing from 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, detection, investigation or prosecution of terrorist offences and organised crime[39]. The Passenger Information Units of the receiving Member States shall (...)[40] transmit the PNR data to their relevant competent authorities (...).

---

[38] At the suggestion of several delegations (FR, HU, SE), the Presidency proposes to delete this provision from the draft Framework Decision. As air carriers have the option to use intermediaries or not, these intermediaries simply exercise the obligations of air carriers, but obviously cannot exempt the air carriers from their obligations. Therefore it does not deem expedient to regulate their obligations separately. The Presidency suggests to insert a new recital (17a) to clarify that air carriers may transmit the PNR data through designated intermediaries.

[39] Several delegations (CZ, EE, UK) indicated they wanted the purpose limitation to be broadened. The Presidency suggests this question will be dealt with in the context of the general debate on the scope of the Framework Decision and also refers to the suggestion it has made with regard to the definition of organised crime in Article 2(i).

[40] At the suggestion of DE, the Presidency has deleted the reference to the retention period. The Presidency shares the view that the retention period set out in Article 9 should apply only to raw PNR data held by the PIU and not to analysed PNR data which have been transmitted onwards for further use.

2. The Passenger Information Unit or any of the (...) competent authorities[41] of a Member State shall have the right to request, either on an ad hoc or on a regular basis[42], the Passenger Information Unit of any (…)[43] Member State to provide it with specific PNR data which are kept in the latter's active database as per Article 9(1), and, where appropriate, analytical data related to such specific PNR data. The request for such data may be based on any one or a combination of data elements, as deemed appropriate by the requesting Unit or competent authority for the prevention, detection, investigation or prosecution of terrorist offences and organised crime. Passenger Information Units shall respond to such requests as soon as practicable[44].

---

41 LT objected to the possibility of the competent authorities of other Member States to request directly a PIU from another Member State. It thought all communication should take place between PIUs. The Presidency invites other delegations to make known their view on this. The UK pleaded in favour of allowing the competent authorities of different Member States to exchange PNR data between each other. The Presidency thinks this is allowed under the international police or judicial co-operation and should not be addressed specifically in this provision. It suggests an additional recital 21a to clarify this.

42 The Commission representative clarified that this paragraph could also be used to make a regular, standing request to the PIU of another Member State for certain type of PNR data.

43 Presidency suggests to delete the word 'other' so as to encompass the possibility for a competent authority to request PNR data from its own PIU. The presidency acknowledges that eventually this may be better regulated in a different provision.

44 UK suggestion so as not to render the obligation on the requested PIU too onerous. SE thought these requests should be governed by the Framework Decision of 18 December on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. The Presidency thinks that the question whether the latter Framework Decision, including the strict time limits laid down therein, can be made applicable to the exchange of PNR data between PIUs merits further reflection.

3. When a PIU or a competent authority of a Member State requests specific PNR data of another Member State which are kept in a dormant database as per Article 9(2), the request shall be made to the Passenger Information Unit of that Member State. Such request shall be made only in exceptional circumstances[45] in response to a specific (…)[46] threat related to the prevention, detection, investigation or prosecution 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[47] threat related to the prevention, detection, investigation or prosecution 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.

---

45 At the request of PT, COM clarified that it was for the requesting Member State to assess the exceptional nature of such circumstances.

46 At the request of several delegations (MT, UK) the word 'actual' was deleted. HU scrutiny reservation on deletion.

47 MT and UK thought the term "actual" should be deleted as it made the requirement too stringent.

Article 8

Transfer of Data to Third Countries[48]

1. (…) PNR data and analytical information flowing from PNR data may be provided by a [PIU/Member State] to law enforcement authorities of third countries only if the [PIU/Member State[49]] is satisfied that:

   (a) the authorities of the third country shall use the data only for the purpose of preventing, detecting, investigating or prosecuting of terrorist offences and organised crime[50],

   (b) the receiving authority in the third country is responsible for the prevention, investigation, detection or prosecution of terrorist offences and organised crime or the execution of criminal penalties imposed for such offences,

   (c) in case the PNR data were obtained from another Member State, that Member State has given its consent to transfer in compliance with its national law,

   (d) the third country ensures an adequate level of protection for the intended data processing; and

   (e) the third country shall not transfer the data to another third country without the express consent of the Member State[51].

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.

---

48 HU scrutiny reservation. ES and FI linguistic reservation.

49 The Presidency thinks that there is a general question whether the data protection chapter ass well as Article 8 of the PNR Framework decision should apply solely to PNR data held by PIUs or also to PNR data transmitted to competent authorities.

50 The question of the purpose limitation should be dealt with in the context of the general debate regarding the scope of the PNR FD. The Presidency also refers to the suggestion it has made with regard to the definition of organised crime in Article 2(i).

51 Further to the comments by several delegations (BE, FI) the Presidency has endeavoured to make this provision more precise, by copying the relevant provisions from Article 14 of the draft Framework Decision on data protection.

Article 9

Period of data retention[52]

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 at the Passenger Information Unit for a further period of eight years[53]. During this period, the PNR data may be accessed, processed and used only with the approval of the Passenger Information Unit and only in exceptional circumstances in response to a specific and actual[54] threat or risk related to the prevention, detection, investigation and prosecution 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.

---

52 DE: scrutiny reservation on the collection and processing of personal data in the absence of concrete suspicions. Provided this question is solved in a satisfactory way, DE -in order to accommodate some concerns by other delegations - would suggest to examine an alternative wording according to which the retention period in paragraph 1 might be drafted as a minimum standard, allowing Member States to provide longer retention periods
under national law. The Presidency thinks this should be discussed in the context of the debate with the Parliament..

53 Some Member States thought this period was too long. The Presidency invited delegations to reflect on the appropriate time period required. The Presidency thinks this should be discussed in the context of the debate with the Parliament.

54 MT and UK argued in favour of a lower threshold without need to demonstrate the actual nature of the threat.

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

4. (…)[55].

Article 10

Sanctions[56]

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, with regard to PNR data collected by them, do not transmit all data required under this Framework decision or do not do so in the require format or otherwise infringe the national provisions adopted pursuant to this Framework Decision[57]. (…)[58]

---

55 COM clarified that the retention periods applied only to the PNR data held by PIUs, not to PNR data transferred to competent authorities. The Presidency agrees with the remark by several delegations (BE, CY, CZ, ES, LU and PL) that the retention of PNR data and their treatment should not be regulated in the PNR FD, but should be left to general data protection principles. Paragraph 4 has consequently been deleted.

56 HU scrutiny reservation.

57 HU and PL thought that air carriers could at any rate not be sanctioned for incomplete or erroneous PNR data. The presidency has endeavoured to ally these concerns by amending the drafting.

58 CZ, FR, GR, LV and LU questioned whether it was necessary to list sanctions. The Presidency has accordingly deleted this reference.

CHAPTER III

PROTECTION OF PNR DATA [59]

Article 11

Protection of PNR data

1. Member States shall ensure that all processing of PNR data pursuant to this Framework Decision , by the Passenger Information Unit or by an air carrier, takes place in accordance with the provisions of Articles 11-12.

2. PNR data which is received pursuant to this Framework Decision by the Passenger Information Units (...) and the designated competent authorities of all the Member States shall exclusively be processed for the purposes set out in Articles 3(3)(4) and 4(4)(5). Processing of the data must be legitimate and adequate, relevant and not excessive.

3. This Framework Decision shall not preclude Member States from providing at national level, higher safeguards for the protection of PNR data , than those established in Articles 11-12.

[59] EE, ES, IT and HU scrutiny reservation on the revised provisions of this chapter.

Article 11a

Processing of special categories of data[60]

In addition to the guarantee set out in Article 3(3) *in fine*, Member States shall ensure that the processing, by Passenger Information Units of PNR data , may not be based solely on a person's race or ethnic origin, religious or philosophical belief, political opinion[61], trade union membership, health or sexual orientation.

Article 11b

Logging and documentation

1. All transmissions of PNR data by air carriers in accordance with Article 3(3) and all transmissions of PNR data by Passenger Information Units, are to be logged or documented by the PIU for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.

2. These logs shall be kept for a period of [5] years[62].

3 Logs or documentation prepared under paragraph 1 shall be communicated on request to the competent national supervisory authority for the control of data protection. The competent supervisory authority shall use this information only for the control of data protection and for ensuring proper data processing as well as data integrity and security.

---

60 CZ and HU questioned the use of the term 'special categories of data'.

61 CZ thought that political opinion could be a valid ground for processing in the context of the fight against terrorism.

62 EE pointed out that there might be a need to specify a period for retaining logs.

Article 11c

Information for the data subject

Member States shall ensure that air carriers inform passengers of international flights about the provision of PNR data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and organised crime, about the possibility of exchanging and sharing of such data and about their rights in accordance with Articles 11d to 11g[63].

Article 11d

Right of access[64]

1. Every data subject is entitled, on request made at reasonable intervals, to receive without constraint and without excessive delay or expense:

   (a) at least a confirmation from the Passenger Information Unit or from the national supervisory authority as to whether or not PNR data relating to him or her have been transmitted to a competent authority, communication of the PNR data undergoing processing and, where possible[65], information on this competent authority; or

   (b) at least a confirmation from the national supervisory authority that all necessary verifications have taken place.

---

63 Several delegations (AT, BE, CZ, DE, EE, ES, FI, HU, NL and UK) pleaded in favour of informing passengers about their rights under the PNR Framework decision.

64 CZ and PT scrutiny reservation

65 DK and UK thought this might be problematic in view of the so-called 'neither confirm, neither deny' policy used in some instances with regard to personal data transmitted to security services.

2. The Member States may adopt legislative measures restricting access to information pursuant to paragraph 1(a), where such a restriction, with due regard for the legitimate interests of the data subject, constitutes a necessary and proportional measure:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) for protecting public security;

(d) for protecting national security;

(e) for protection of the data subject or of the rights and freedoms of others.

3. Any refusal or restriction of access shall be set out in writing to the data subject. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him. This communication may be waived where a reason pursuant to paragraph 2, points (a) to (e), exists. In all of these cases the data subject shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court.

Article 11e

Right to rectification and erasure[66]

1. With regard to PNR data , the Passenger Information Unit shall:

   - where it is aware that such data are incorrect, rectify such data if they are inaccurate;

   - where possible and necessary, complete or update such data; and

   - where such data have been made available by the air carriers in violation of the national provisions adopted pursuant to this Framework Decision, erase such data .

2. Member States shall lay down whether the data subject can assert these rights directly against the Passenger Information Unit or through the intermediary of the competent national supervisory authority. If the Passenger Information Unit refuses rectification or erasure of such data, the refusal must be communicated in writing and the data subject informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy. When the complaint or judicial remedy is examined, the data subject shall be informed whether the Passenger Information Unit acted properly or not. Member States may also provide that the data subject shall only be informed by the competent national supervisory authority that a review has taken place.

---

[66] PT scrutiny reservation. CZ and DE queried whether the PNR Framework decision should allow for the referencing or blocking of data. The Presidency is interested in hearing other delegation' views on this, but wondered what would be the practical value of such possibility in this context where PNR data are generated by data subjects themselves and provided to air carriers - under the 1995 Data Protection Directive, they have the right to have those data corrected by the air carriers. The Presidency also reminds delegations of the fact that such a possibility, if it were to be included, here might be prone to misuse by passengers who deliberately provide incorrect data to air carriers.

Article 11f

Right to compensation[67]

1. Member States shall ensure that any data subject who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision is entitled to receive compensation from the Member State responsible for the damage suffered.

2. Member States shall ensure that any data subject who has suffered damage as a result of a transmission of PNR data by the air carriers in violation of the national provisions adopted pursuant to this Framework Decision, is entitled to receive compensation from air carrier under national law for the damage suffered.

Article 11g

Judicial remedies

Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject must have the right to seek judicial remedy for any breach of the rights guaranteed to him by the national provisions adopted pursuant to this Framework Decision.

---

67 PT scrutiny reservation. DE thought that the compensation mechanism provided for under Article 19(2) DPFD could be made applicable in this context as well by way of a constituent reference. The Presidency respectfully disagrees with this. Article 19(2) DPFD is concerned with an inter-State reimbursement mechanism, wheras the situation here is one of the relation between a private actor which is obliged to provide data to national authority (PIU). The Presidency deems that the question whether and how a PIU can ask for the reimbursement of compensation it has been obliged to pay as the result of a fault of an air carrier, is something which can be left to national law.

Article 11h

Confidentiality of processing

1. Persons who have access to PNR data, held by Passenger Information Units, may process such data only as members or on the instructions of the relevant Passenger Information Unit, unless there are legal obligations to do so.

2. Persons called upon to work for a Passenger Information Unit of a Member State shall be bound by all the data protection rules which apply to the Passenger Information Unit in question.

Article 11i

National Supervisory Authority

1. Without prejudice to wider powers under national law, each Member State shall provide that a public authority is responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Chapter[68]. These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each authority shall be endowed in particular with:

(a) investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

[68] The Presidency thinks that Articles 8 (exchange with third countries) and 9 (retention period) should also be placed in this chapter, as they are data protection related. This would enable the supervisory authorities to control these aspects as well.

(b) effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

(c) the power to engage in legal proceedings where the national provisions adopted pursuant to this Chapter have been infringed or to bring such infringements to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

3. Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

4. Member States shall provide that the members and staff of the supervisory authority are also to be bound by the data protection provisions applicable to the competent authority in question and, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

5. Each Member State shall notify the Commission and the General Secretariat of the Council, by way of a declaration, the supervisory authority it has designated for the purposes of this Framework Decision. Such declaration shall be made 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 12

Data security

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

a) physically protect data;

b) deny unauthorised persons access to national installations in which the Passenger Information Units 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 PNR data (storage control);

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

f) ensure that, within the Passenger Information Units, persons authorised to access the PNR 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) (...);

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

i) prevent the unauthorised reading and copying of PNR 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