



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 23 January 2009

5618/09

**Interinstitutional File:
2007/0237 (CNS)**

**CRIMORG 7
AVIATION 3
DATAPROTECT 2**

NOTE

from : Presidency

to : Multidisciplinary group on organised crime

No. prev. doc. : 7656/3/08 CRIMORG 49 AVIATION 77 DATAPROTECT 14
16457/08 CRIMORG 208 AVIATION 286 DATAPROTECT 100 +
COR 1 + COR 2

Subject : Proposal for a Council Framework Decision on the use of Passenger Name
Record (PNR) for law enforcement purposes

The Commission submitted the above proposal for a framework decision to the Council on 17 November 2007 and 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. During the Slovenian Presidency three readings of the proposal took place.

During the French Presidency, a thematic approach was followed and the most important themes surrounding the possible introduction of a system of collecting and processing PNR data in the European Union were studied in depth. The results of these discussions in the MDG are set out in three outcomes of proceedings.¹ The result of these discussions were also discussed twice at ministerial level by the Council, on 25 July and 27 November 2008².

At its meeting of 27 November 2008, the Council instructed the preparatory bodies of the Council “to examine all the outstanding issues, whether legal or operational, in the light of the report and all the work already carried out with a view to possible decisions at a later date”. This Presidency has sought to follow this instruction by endeavouring to incorporate the main findings at which the MDG arrived during the French Presidency into the text of the draft Framework decision, as it stood at the end of the Slovenian Presidency³. The attached text therefore introduces a significant number of changes which, in the Presidency’s view, fairly translate these MDG findings; while bearing in mind that not all these results were supported by all delegations. The Presidency has also, again based on the excellent work carried out during the French Presidency, incorporated some proposals that were made with regard to items on which clearly no consensus has been reached yet, like the retention period and the use of sensitive data.

The text set out in 7656/3/08 CRIMORG 49 AVIATION 77 DATAPROTECT 14 was subject to a large number of reservations: AT reservation; general scrutiny reservation on the proposal by BE, BG, CZ, DK, FI, HU, IT, LU, LV, LT, MT, PL, PT 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.

¹ 13319/08 CRIMORG 144 AVIATION 187 DATAPROTECT 62; 13860/08 CRIMORG 159 AVIATION 216 DATAPROTECT 71 and 15441/08 CRIMORG 188 AVIATION 260 DATAPROTECT 89.

² 13803/1/08 CRIMORG 157 AVIATION 211 DATAPROTECT 70 and 16457/08 CRIMORG 208 AVIATION 286 DATAPROTECT 100 + COR 1+ COR 2.

³ 7656/3/08 CRIMORG 49 AVIATION 77 DATAPROTECT 14.

The Presidency understands that the attached text, given that it is an overhaul of the previous text, is generally subject to scrutiny by all delegations. Delegations are also invited to check the footnotes so as to verify whether the reservations mentioned there are still valid. Obviously a number of footnotes featuring in 7656/3/08 CRIMORG 49 AVIATION 77 DATAPROTECT 14 have disappeared, as the text which they accompanied has been changed.

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 Commission⁴,

Having regard to the opinion of the European Parliament⁵,

Whereas,

- (1) The European Council adopted the Declaration on combating terrorism on 25 March 2004⁶ inviting the Commission to bring forward, inter alia a proposal for a common EU approach to the use of passenger's 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 Programme⁷ and at the extraordinary Council meeting of 13 July 2005⁸.

⁴ OJ

⁵ OJ

⁶ 7906/04.

⁷ The Hague Programme – Strengthening Freedom, Security and Justice in the European Union, paragraph 2.2 Terrorism.

⁸ 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 serious crime, be carried out in an adequate manner. The definitions of terrorist offences and serious crime are taken from Articles 1 to 4 of the Council Framework Decision 2002/475/JHA on combating terrorism⁹ and Article 2 of the Council Framework Decision on the European Arrest Warrant and the surrender procedures between Member States¹⁰ respectively.
- (4) Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data¹¹ regulates the transmission of advance passenger information (API) 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 terrorist offences and serious crime and thus to enhance internal security. The use of PNR data together with API data in certain cases has added value in assisting Member States in verifying the identity of an individual;
- (5a) This Framework Decision shall not apply to activities which fall outside the scope of Title VI of the Treaty on European Union, such as those covered by the Treaty establishing the European Community or national law.

⁹ OJ L 164, 22.6.2002, p. 3.

¹⁰ OJ L 190, 18.7.2002, p.3

¹¹ OJ L 261, 6.8.2004, p. 24.

- (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.
- (7) To prevent, detect, investigate and prosecute terrorist offences and serious 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, including those segments connecting two EU-airports which are part of an international flight. Member States may chose to include intra-EU flights in their national PNR systems, but such flights should, at this stage, not be covered by this Framework Decision. The experiences of those Member States may, however, be drawn upon in the context of a future reflection on the extension of the scope of the Framework Decision.
- (7a) This Framework decision does not derogate from Member States' right to provide, under their domestic law, for a system of collection and handling of PNR data for other purposes than those specified in this Framework decision, or from other transportation providers than those specified in the Framework decision. In such cases, appropriate data protection regimes shall apply, such as the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- (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 serious 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 serious crime. Because of the nature of the data and its uses, it is important that the data is kept for a sufficiently long period for carrying out trend analysis and for using in investigations. In order to avoid a disproportionate use, it is important that after some years, the data is archived and only accessible under very strict and more limited conditions. At the same time this ensures that it is available if it is needed in specified exceptional circumstances, as well as for trend analysis.
- (10) Data protection rules applicable to all PNR data processed by the Passenger Information Units 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 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 of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (2008/977/JHA), as is the exchange of PNR data between the competent authorities of various Member States¹².

¹² CZ and PL suggested to put this into the body of the text.

- (10b) The processing of PNR data by competent authorities is equally subject to the data protection safeguards laid down in the Council Framework Decision of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (2008/977/JHA) or to national data protection rules which match those data protection safeguards and, in respect of Member States who have ratified the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, having regard to the provisions of that Convention and taking into account Recommendation No R(87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the use of Personal Data in the Police Sector. However, it is necessary to specify the rules regarding the (...) use of PNR data in this Framework decision.
- (11) To ensure the effectiveness of the obligations on air carriers to transfer or 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) It is necessary that competent national authorities are provided with PNR data which is 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 serious crime.

- (15) The Commission in its Communication of 16 December 2003 on “Transfer of air PNR data: a global EU-approach”¹³ 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.
- (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 transfer or 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 Decision¹⁴.

¹³ COM(2003) 826, 16.12.2003.

¹⁴ ES scrutiny reservation.

- (18) The contents of any lists of required PNR data to be obtained by the Passenger Information Units should reflect an appropriate balance between the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences and serious crime, thereby improving the internal security within the EU and the protection of fundamental rights of citizens, notably privacy.
- (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 serious 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 results of the processing of PNR data that they receive as necessary. Transfers of PNR data by a Member State to third countries should be permitted only on a case-by-case basis and subject to additional requirements relating to the purpose of the transfer, the quality of the receiving authority and the level of data protection in the third country. Where the Member States or the Union has entered into international agreements on such transfers before the entry into force of this Framework Decision, the provisions of such agreements should apply.
- (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, including through Eurojust and Europol, which 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 (...) 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 and readability of the data transmitted. The standards which are recommended by IATA should be taken into consideration in achieving secure transmissions of the data.
- (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 transfer or the making available by air carriers of PNR data of passengers of international flights to the Member States, for the purpose of preventing detecting, investigating and prosecuting terrorist offences and serious crime, as well as the processing of those data, including their collection, use and retention by the Member States 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. The obligations under this Framework Decision shall be incumbent on the air carrier also in the event that the air carrier designates an intermediary for the purposes related to this Framework Decision ¹⁶;
- (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 and includes charter flights and air taxis;

¹⁵ CZ and SE scrutiny reservation.

¹⁶ COM indicated that the current definition covered so-called air taxis, but excludes purely private flights. Cargo flights would be excluded, as they normally do not gather PNR data. The question to what extent data collected by code-sharing air carriers would be governed by this instrument, would be further examined by the Commission.

- (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), or equivalent systems providing the same functionalities. 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 carrier;
- (d) 'passenger' means any person, except members of the crew¹⁷, 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 for the handling of reservations ;
- (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 (...) and equivalent system and extract the required data into their database;
- (g) "terrorist offences" means the offences under national law, referred to in Articles 1 to 4¹⁸ of the Council Framework Decision 2002/475/JHA on combating terrorism;
- (h) "serious crime" means the offences under national law, referred to in Article 2 of the Council Framework Decision on the European Arrest Warrant and the surrender procedures between Member States if they are punishable by a custodial sentence or a detention order [for a maximum period of at least three years under national law].

¹⁷ UK wanted to include crew members.

¹⁸ BE thought it was sufficient to mention Article 2 and it was not necessary to include Articles 1, 3 and 4.

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 3

Passenger Information Unit¹⁹

1. Each Member State shall set up or designate a public authority or a branch of such an authority to act as its "Passenger Information Unit "responsible for collecting the PNR data from the airlines, store them, analyse them and transmit the result of the analysis to the competent authorities. Its staff members may be detached from [various/competent] public authorities. 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*.
2. The Passenger Information Unit shall be responsible for collecting the PNR data from 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 beyond those listed in the Annex, the Passenger Information Unit shall delete such data immediately upon its receipt.

¹⁹ CZ and DE scrutiny reservation.

3. The Passenger Information Unit shall process PNR data only for the following purposes:

- (a) carrying out real time risk assessment of the passengers²⁰ in order to identify the persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities of the Member State, referred to in Article 4. In carrying out such risk assessments, the Passenger Information Unit may process PNR data against pre-determined risk criteria and against relevant databases, in accordance with European, international and national rules applicable to such databases. A positive match as a result of such automated processing shall be manually reviewed by the Passenger Information Unit in order to verify whether these need to be transmitted to the competent authority referred to in Article 4 with a view to preventing, detecting, investigating or prosecuting terrorist offences and serious crime;
- (b) responding, on a case-by-case basis, to requests from competent authorities to provide PNR data and process PNR data in a specified manner and to provide the competent authorities with the results of such processing. Such requests shall relate to a specific investigations or prosecutions concerning a terrorist offences and serious crime and must be reasoned; and
- (c) analysing PNR data for the purpose of identifying trends and updating or creating new risk criteria for carrying out risk assessments according to paragraph (a).

²⁰ Some delegations have pleaded in favour of some degree of harmonisation with regard to the risk assessment: AT, LU, PT, SK.

4. The criteria and guarantees in respect of real time risk assessments referred to in paragraph 3(a) will be provided for under national law, taking due account of the recommendations for common general criteria, methods and practices for risk assessments which shall be adopted under the procedure of Articles 13, 14 and 15. Member States shall ensure that the risk criteria shall be set by the competent authorities referred to in Article 4 and shall in no circumstances be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual orientation.
5. The transmission by the Passenger Information Unit of a Member State of the PNR data of the individuals identified in accordance with paragraph 3(a), (b) and (c) for further examination to the relevant competent authorities of the same Member State shall take place by electronic means or, in case of technical failure, by any other appropriate means²¹. (.....)
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 Unit shall be established in one of the participating Member States and shall be considered the national Passenger Information Unit of all such participating Member States²². 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.

²¹ HU indicated telex might be used. SE asked for the deletion of alternative means. UK scrutiny reservation.

²² 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 request or receive PNR data or analysis²³ of PNR data from the Passenger Information Units in order to examine this information further or take appropriate action.
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 serious 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 and the analysis of PNR data by the Passenger Information Unit may be further processed by the competent authorities of the Member States only with the aim of preventing, detecting, investigating or prosecuting terrorist offences and serious 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 enforcement action further to such processing²⁴.
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 the 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.

²³ DK scrutiny reservation on the inclusion of the analysis of PNR data.

²⁴ CZ scrutiny reservation.

Article 5

Obligation on air carriers²⁵

1. Member States shall adopt the necessary measures²⁶ to ensure that air carriers transfer or 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 an international flight is code-shared between one or more air carriers, the obligation to transfer or to make available the PNR data of all passengers of the flight should be on the air carrier that operates the flight. In cases in which a transiting international flight includes a segment involving two or more different Member States, air carriers should transfer or make available the PNR data of the passengers to the Passenger Information Units of all the involved Member States²⁷.

- 1a. Within [6] years following [the date referred to in Article 16] Member States shall ensure that the PNR data with regard to all flights referred to in paragraph 1 are collected. In the interim period up to that date, Member States may provide that PNR data are collected only with regard to those flights that they consider to be risk flights. In the first half of the interim period up to [3] years following [the date referred to in Article 16], those risk flights shall constitute, on a yearly basis, no less than [30] % of all flights referred to in paragraph 1 and in the second half of the interim period between [3] and [6] years following [the date referred to in Article 16], those risk flights shall constitute, on a yearly basis, no less than [60] % of all flights referred to in paragraph 1.

²⁵ CZ scrutiny reservation.

²⁶ PL reservation on paragraph 1. PL in particular queried the meaning of 'necessary measures'.

²⁷ LT reservation: unacceptable to oblige air carriers to provide data to more than one Member State. This 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.

2. Air carriers shall transfer or make available to the Passenger Information Unit the PNR data specified in the Annex to the extent that it is kept at the air carrier's disposal.
3. Air carriers shall transfer or make available twice such data by electronic means using the common protocols and supported data formats to be adopted according to the procedure of Articles 13, 14 and 15, or, in case of technical failure, by any other appropriate means:
 - (a) once in advance, not more than 48 and not less than 24 hours before the scheduled time for flight departure, at a time chosen by the air carrier

and

- (b) once immediately after flight closure, that is immediately after the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board. Member States shall permit air carriers to limit this transfer or making available to updates of the first transmission.

In specific cases, when there is an indication that early access is necessary to assist in responding to a specific and actual threat related to terrorist offences and serious crime, a Passenger Information Unit may, in accordance with national law²⁸, require an air carrier to transfer or to make available to it PNR data prior to 48 hours from the scheduled time for flight departure. (...)

4. Following the expiry of a transition period of [three] years after the [the date referred to in Article 16 (1)]], all air carriers shall be required to use the "push method" to transfer the data to the Passenger Information Units. During the transition period, air carriers that 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".

²⁸ This addition was made 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.

5. Member States shall ensure that air carriers [, travel agencies and ticket sellers] inform passengers in accordance with Article 11c of this Framework Decision.

Article 6
Intermediary

Article 7
Exchange of Information between Member States

1. Member States shall ensure that the PNR data or analysis of PNR data²⁹ with regard to persons identified by a Passenger Information Unit in accordance with Article 3(3)(a) 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 serious crime. The Passenger Information Units of the receiving Member States shall transmit such PNR data to their relevant competent authorities.

²⁹ CZ and HU scrutiny reservation.

2. The Passenger Information Unit of a Member State shall have the right to request, either on an ad hoc or on a regular basis³⁰, the Passenger Information Unit of any other Member State to provide it with PNR data which are kept in the latter's database as per Article 9(1), and, where appropriate, to request the processing of PNR data in a specified manner and the provision of the results of such processing. 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, detection, investigation or prosecution of terrorist offences and serious crime. Passenger Information Units shall respond to such requests as soon as practicable³¹.
- 2a. The competent authorities³² of a Member State shall have the right to request, on a case-by-case basis, the Passenger Information Unit of any other Member State to provide it with PNR data which are kept in the latter's database as per Article 9(1), and to request the processing of PNR data in a specified manner and the provision of the results thereof. Such requests shall relate to specific investigations or prosecutions of terrorist offences and serious crime. Passenger Information Units shall respond to such requests as soon as practicable.

³⁰ COM 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.

³¹ CZ scrutiny reservation. SE thought these requests should be governed by the Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. 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.

³² 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.

3. When a Passenger Information Unit or a competent authority of a Member State requests specific PNR data of another Member State which are kept in archives 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 circumstances³³ in response to a specific threat or a specific investigation or prosecution related to the prevention, detection, investigation or prosecution of terrorist offences and serious crime.
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, detection, investigation or prosecution of terrorist offences and serious crime, the Passenger Information Unit of a Member State or the (...) 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 48 hours before the scheduled time for flight departure.

Article 8

Transfer of Personal Data to Third Countries³⁴

1. PNR data and the analysis of PNR data may be transferred or made available by a Member State to a third country only on a case-by-case basis and only if the Member State is satisfied that:
 - (a) the transfer is necessary for the purpose of preventing, detecting, investigating or prosecuting of terrorist offences and serious crime;
 - (b) the receiving authority in the third country is an authority responsible for the prevention, investigation, detection or prosecution of terrorist offences and serious crime (...);

³³ COM clarified that it was for the requesting Member State to assess the exceptional nature of such circumstances.

³⁴ CZ and HU scrutiny reservation. ES linguistic reservation.

- (c) in case the PNR data was obtained from another Member State, that Member State has given its consent to the 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.
2. By way of derogation from paragraph 1(c), data may be transferred to a third country without the prior consent of the Member State from which the data was obtained only if the transfer of the data is essential for the prevention of an immediate and serious threat related to the prevention, detection, investigation or prosecution of terrorist offences and serious crime, and the prior consent cannot be obtained in time. The transferring Member State shall inform the Member State from which the data was obtained without delay.
3. The adequacy of the level of protection referred to in paragraph 1(d) shall be assessed in the light of all the circumstances surrounding the data transfers. Particular consideration shall be given to the purpose of the use of the data, the data retention period, the country of final destination of the data, the rule of law in force in the third country and its security measures.

4. 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 retention³⁵

1. Member States shall ensure that the PNR data provided by the air carriers to the Passenger Information Unit are kept in a database at the Passenger Information Unit for a period of three 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 three years of the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be archived at the Passenger Information Unit for a further period of [not less than three and not more than seven] years. During this period, the PNR data may be accessed, processed and used only by specially authorised personnel of the Passenger Information Unit, who have received a specific training regarding the applicable legislation on the collection and use of PNR data. Access shall be permitted only in response to a specific and actual³⁶ threat or risk or a specific investigation or prosecution or for analytical purposes related to the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
3. Member States shall ensure that the PNR data is deleted from all the databases of their Passenger Information Unit upon the expiry of the period specified in paragraph 2.

³⁵ DE scrutiny reservation on the collection and processing of personal data in the absence of concrete suspicions.

³⁶ MT and UK argued in favour of a lower threshold without need to demonstrate the actual nature of the threat.

3a. The result of matching referred to in Article 3(3)(a) shall be kept by the Passenger Information only as long as necessary to inform the competent authorities of a positive match. Where the result of an automated matching operation has, further to manual verification, proven to be negative, it may, however, be stored so as to avoid future "false" positive matches [for a maximum period of three years].

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 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 required format or otherwise infringe the national provisions adopted pursuant to this Framework Decision.

CHAPTER III

PROTECTION OF PNR DATA

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, takes place in accordance with the provisions of Articles 11-12;
 - all processing of personal data pursuant to this Framework Decision by the competent authorities is subject to a standard of protection of personal data under its national law which at least corresponds to the standards of the Council Framework Decision of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters (2008/977/JHA) and has regard to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data, taking into account Recommendation No R(87)15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the use of Personal Data in the Police Sector.
2. PNR data which is received pursuant to this Framework Decision by the Passenger Information Units and the competent authorities of all the Member States shall exclusively be processed for the purposes set out in Articles 3(3) 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.

Processing of special categories of data³⁷

1. Processing by Passenger Information Units of PNR data revealing a person's race or ethnic origin, religious or philosophical belief, political opinion³⁸, trade union membership, health or sexual orientation shall only be carried out on a case by case basis and when the following conditions are met:
 - (a) in the case of an automated risk assessment referred to in Article 3(3)(a), following completion thereof;
 - (b) where strictly necessary for an ongoing investigation or prosecution related to the prevention, detection, investigation or prosecution of one or more terrorist offences and/or one or more serious crimes; and
 - (c) when domestic law provides adequate safeguards.
2. Access to the special categories of data referred to in paragraph 1 shall be limited to specially authorised personnel of the Passenger Information Unit, who have received a specific training regarding the applicable legislation on the collection and use of PNR data and who shall access such data manually.

³⁷ CZ and HU questioned the use of the term 'special categories of data'.

³⁸ CZ thought that political opinion could be a valid ground for processing in the context of the fight against terrorism.

Article 11b

Logging and documentation

1. All transmissions of PNR data by air carriers, all transmissions of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States, are to be logged or documented by the Passenger Information Unit 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.
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 security³⁹.

³⁹ SE thought these logs or documentation should also be allowed to use for pressing charges by the supervisory authority. The Presidency thinks this use is covered by the terms 'control of data protection'.

Article 11c

Information for the data subject

1. 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 serious crime, about the possibility of exchanging and sharing of such data and about their rights in accordance with Articles 11d to 11g⁴⁰.
2. Member States shall ensure that all information referred to in paragraph 1 is also available in a clear, precise manner through a guide on passengers' rights of access and through posters at the airport.

Article 11d

Right of access⁴¹

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 possible⁴², information on this competent authority; or

⁴⁰ CZ scrutiny reservation.

⁴¹ CZ and PT scrutiny reservation.

⁴² 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.

- (b) at least a confirmation from the national supervisory authority that all necessary verifications have taken place.
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 erasure⁴³

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 transferred or 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.

⁴³ CZ and PT scrutiny reservation. CZ and SE queried whether the PNR Framework decision should allow for the referencing or blocking of data.

Article 11f

Right to compensation⁴⁴

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 suffered⁴⁵.

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.

⁴⁴ PT scrutiny reservation.

⁴⁵ DE scrutiny reservation: DE thought that the compensation mechanism provided for under Article 19(2) DPF⁴⁴ could be made applicable in this context as well by way of a constituent reference. The Presidency respectfully disagrees with this. Article 19(2) DPF⁴⁴ is concerned with an inter-State reimbursement mechanism, whereas 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 processing⁴⁶

1. Persons who have access to PNR data, held by Passenger Information Units, may process such data only as members of the Passenger Information Unit 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 one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Chapter. 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;

⁴⁶ SE asked to change the heading of this provision into: "Persons processing personal data".

- (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) deny unauthorised persons access to equipment used for processing personal data by the Passenger Information Units store data (equipment access control);
- b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
- c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored PNR data (storage control);
- d) prevent the use of automated data processing systems by unauthorised persons using data communication equipment (user control);
- e) 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 (data access control);
- g) ensure that it is possible to verify and establish to which competent authorities PNR data may be transmitted using data communication equipment (communication control);
- h) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data was input (input control);
- i) prevent the unauthorised reading and copying of PNR data during its transmission, in particular by means of appropriate common protocols (transport control);
- j) ensure that installed systems may, in case of interruption, be restored (recovery);

- k) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity);
- l) ensure that the databases are located in adequately secure premises.

CHAPTER IV

COMITOLOGY

Article 13

Common Protocols

1. Until the time limit referred to in paragraph 6 of this Article has elapsed, all transmissions of PNR data by air carriers to the Passenger Information Units made for the purposes of this Framework Decision shall be made by electronic means or, in case of failure, by any other appropriate means, and in a specified data format.
2. Once the time limit referred to in paragraph 6 of this Article has elapsed, all transmissions of PNR data by air carriers to the Passenger Information Units made for the purposes of this Framework Decision shall be made electronically using secure methods in the form of acceptable common protocols which shall be common to all transmissions to ensure the security of the data during transmission, and in a supported data format to ensure their readability by all parties involved. Air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that it intends to use for its transmissions to it.
3. The list of acceptable common protocols and supported data formats 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 support all the acceptable common protocols and data formats.
6. The technical alterations referred to in paragraph 5 shall be carried out within 1 year from the date the common protocols and supported data formats 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 procedure⁴⁷

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 data formats which shall be used in all PNR transmissions by air carriers to the Passenger Information Units under this Framework Decision as well as the common general criteria, methods and practices for the risk assessment according to Article 3(3) (a) and 3(4).

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.

⁴⁷ ES had some doubts on the use of comitology, whereas SE opined this should be looked at again after the entry into force of the Lisbon Treaty. IT scrutiny reservation.

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

Implementation⁴⁸

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision before [31 December 2010]⁴⁹. 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.

⁴⁸ CZ scrutiny reservation.

⁴⁹ PL thought a 36-months transposition period would be required.

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 has been implemented. Such review shall comprise all the elements of this Framework Decision, with special attention to 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. It shall also contain the statistical information gathered pursuant to Article 18. It shall examine in particular the following two questions and contain, if appropriate, recommendations:

- the gradual increase of flights with regard to which PNR data are collected, as referred to in Article 5(1a); and
- the cost-benefit relation between the potential inclusion of intra-community flights in the scope of the Framework Decision, in the light of the national experiences gathered by those Member States that have decided to collect PNR data with regard to intra-community flights.

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 data⁵⁰.
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.

⁵⁰ DK thought it should be further clarified which statistics are required. EE and ES also questioned the detail required under this provision.

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

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 (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)
- (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

All historical changes to the PNR listed in numbers 1 to 18.
