



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 10 October 2011

**Interinstitutional File:
2011/0023 (COD)**

**14233/1/11
REV 1**

LIMITE

**GENVAL 91
AVIATION 207
DATAPROTECT 95
CODEC 1447**

NOTE

from:	Presidency
to:	Working Party on General Matters, including Evaluations
No. prev. doc.:	6007/11 GENVAL 5 AVIATION 15 DATAPROTECT 6 CODEC 278
Subject:	Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Following the discussions in the Working Party on General Matters, including Evaluations (GENVAL) meeting on 30 September 2011 as well as drawing on subsequent written contributions by a number of Member States, delegations find attached a revised version of the Presidency proposal for the PNR Directive (14233/11).

The major change introduced to the text in comparison with the doc.14233/11 is deletion of distinction between 'serious crime' and 'transnational serious crime'. The Presidency suggests to delete the latter category whilst restoring the definition of the former as put forward by the Commission in its initial proposal. Simultaneously delegations are invited to reflect on a list (Annex 2) of relevant serious crime with relation to which PNR data might be used for the creation and application of assessment criteria.

The following delegations maintain a general scrutiny reservation on the proposal: BE, BG, CZ, DE, EE, ES, FI, FR, GR, IE, IT, LT, LV, LU, NL, AT, PT, RO and UK.

The following delegations hold a parliamentary scrutiny reservation: CZ, FR, IE, LT and UK.

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 82(1)(d) and 87(2)(a) thereof,

Having regard to the proposal from the Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee¹,

Having regard to the opinion of the Committee of the Regions²,

After having consulted the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

¹ OJ C , , p. .

² OJ C , , p. .

Whereas:

- (1) On 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes³. However, upon entry into force of the Treaty of Lisbon on 1 December 2009, the Commission's proposal, which had not been adopted by the Council by that date, became obsolete.
- (2) The 'Stockholm Programme — An open and secure Europe serving and protecting the citizens'⁴ calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.
- (3) In its Communication of 21 September 2010 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries'⁵ the Commission outlined certain core elements of a Union policy in this area.
- (4) Council Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data⁶ regulates the transfer of advance passenger information by air carriers to the competent national authorities for the purpose of improving border controls and combating [irregular]⁷ immigration.
- (5) PNR data are necessary⁸ to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security.
- (6) PNR data help law enforcement authorities⁹ prevent, detect, investigate and prosecute serious crimes, including acts of terrorism, inter alia¹⁰ by comparing them with various databases of persons and objects sought, to construct evidence and, where relevant, to find associates of criminals and unravel criminal networks.

³ COM(2007) 654.

⁴ Council document 17024/09, 2.12.2009.

⁵ COM(2010) 492.

⁶ OJ L 261, 6.8.2004, p. 24.

⁷ GR would like to replace „irregular” with „illegal”.

⁸ AT scrutiny reservation.

⁹ SE requests to extend the scope of the recital so as to encompass also intelligence gathering.

¹⁰ UK and SE requested to extend the scope of this recital to be in line with Article 4.

- (7) PNR data enable law enforcement authorities to identify persons who were previously "unknown", i.e. persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved in such crime and who should therefore be subject to further examination by the competent authorities. By using PNR data law enforcement authorities can address the threat of serious crime and terrorism from a different perspective than through the processing of other categories of personal data. However, in order to ensure that the processing of data of innocent and unsuspected persons remains as limited as possible, the aspects of the use of PNR data relating to the creation and application of assessment criteria should be further limited to terrorist offences and relevant forms of serious crime.
- (8) The use of PNR data together with Advance Passenger Information data (...) has added value in assisting Member States in verifying the identity of an individual and thus reinforcing their law enforcement value¹¹.
- (9) To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is therefore essential that all Member States introduce provisions laying down obligations on air carriers operating extra-EU flights to or from the territory of the Member States of the European Union and , where necessary, also selected intra-EU flights between Member States of the European Union.
- (10) Air carriers already collect and process PNR data from their passengers for their own commercial purposes. This Directive should not impose any obligation on air carriers to collect or retain any additional data from passengers or to impose any obligation on passengers to provide any data in addition to that already being provided to air carriers.
- (11) The processing of personal data must be proportionate to the specific security goals pursued by this Directive.

¹¹ FR emphasized the importance of this recital for the future discussion on relevant articles of the proposal.

- (12) The definition of terrorist offences should be taken from Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism¹². The definition of serious crime should be taken from Article 2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedure between Member States¹³. The list of relevant serious crime with relation to which PNR data might be used for the creation and application of assessment criteria should be based on Article 2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedure between Member States.
- (13) PNR data should be transferred to a single designated unit (Passenger Information Unit) in the relevant Member State, so as to ensure clarity and reduce costs to air carriers.
- (14) The contents of any lists of required PNR data to be obtained by the Passenger Information Unit should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union as well as protecting the fundamental rights of persons, notably privacy and the protection of personal data. Such lists should not be based on characteristics enumerated in Article 21 of the Charter of Fundamental Rights. The PNR data should contain details on the passenger's reservation and travel itinerary which enable competent authorities to identify air passengers representing a threat to internal security.

¹² OJ L 164, 22.6.2002, p. 3. Decision as amended by Council Framework Decision 2008/919/JHA of 28 November 2008 (OJ L 330, 9.1.2.2008, p. 21).

¹³ OJ L 190, 18.7.2002, p. 1.

- (15) There are two possible methods of data transfer currently available: the ‘pull’ method, under which the competent authorities of the Member 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 transfer (‘push’) the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided. The ‘push’ method is considered to offer a higher degree of data protection and should be mandatory for all air carriers.
- (16) The Commission supports the International Civil Aviation Organisation (ICAO) guidelines on PNR. These guidelines should thus be the basis for adopting the supported data formats for transfers of PNR data by air carriers to Member States. This justifies that such supported data formats, as well as the relevant protocols applicable to the transfer of data from air carriers should be adopted in accordance with the examination procedure foreseen in Regulation (EU) No182/2011 of the European Parliament and of the Council of 16 February 2011 laying down rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers¹⁴.
- (17) The Member States should take all necessary measures to enable air carriers to fulfil their obligations under this Directive. Dissuasive, effective and proportionate penalties, including financial ones, should be provided for by Member States against those air carriers failing to meet their obligations regarding the transfer of PNR data.
- (18) Each Member State should be responsible for assessing the potential threats related to terrorist offences or and serious crime.

¹⁴ OJ L 55, 28.02.2011, p. 13

- (19) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or seriously affects him/her should be taken only by reason of the automated processing of PNR data. Moreover, no such decision should be taken by reason of a person's characteristics enumerated in Article 21 of the Charter of Fundamental Rights.
- (20) Member States should share with other Member States the PNR data that they receive where such transfer is necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime . The provisions of this Directive should be without prejudice to other Union instruments on the exchange of information between police and judicial authorities, including Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)¹⁵ and Council Framework Decision 2006/960/JHA of 18 September 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union¹⁶. Such exchange of PNR data between law enforcement¹⁷ and judicial authorities should be governed by the rules on police and judicial cooperation.
- (21) The period during which PNR data are to be retained should be proportionate to the purposes of the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data are retained for a sufficiently long period for carrying out analysis and for use in investigations. In order to avoid disproportionate use, it is necessary that, after an initial period, the data are masked out¹⁸ and only accessible under very strict and limited conditions.

¹⁵ OJ L 121, 15.5.2009, p. 37.

¹⁶ OJ L 386, 29.12.2006, p. 89.

¹⁷ SE requests to extend the scope of the recital so as to encompass also intelligence gathering.

¹⁸ BE and FR await explanations as to the notion of masking out.

- (22) Where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, the retention of such data by the competent authority should be regulated by the national law of the Member State, irrespective of the retention periods set by this Directive.
- (23) The processing of PNR data domestically in each Member State by the Passenger Information Unit and by competent authorities should be subject to a standard of protection of personal data under their national law which is in line with Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters¹⁹ (‘Framework Decision 2008/977/JHA’).
- (24) Taking into consideration the right to the protection of personal data, the rights of the data subjects to processing of their PNR data, such as the right of access, the right of rectification, erasure and blocking, as well as the rights to compensation and judicial remedies, should be in line with Framework Decision 2008/977/JHA.
- (25) Taking into account the right of passengers to be informed of the processing of their personal data, Member States should ensure they are provided with accurate information about the collection of PNR data and their transfer to the Passenger Information Unit.
- (26) Transfers of PNR data by Member States to third countries should be permitted only on a case-by-case basis and in compliance with Framework Decision 2008/977/JHA. To ensure the protection of personal data, such transfers should be subject to additional requirements²⁰ relating to the purpose of the transfer, the quality of the receiving authority and the safeguards applicable to the personal data transferred to the third country.

¹⁹ OJ L 350, 30.12.2008, p. 60.

²⁰ GR requested to add clarification to the recital on phrase “additional requirements”.

- (27) The national supervisory authority that has been established in implementation of Framework Decision 2008/977/JHA should also be responsible for advising on and monitoring of the application and implementation of the provisions of this Directive.
- (28) This Directive does not affect the possibility for Member States to provide, under their domestic law, for a system of collection and handling of PNR data for purposes other than those specified in this Directive, or from transportation providers other than those specified in the Directive, provided that such domestic law respects the Union acquis.
- (29)²¹ This Directive is without prejudice to the current EU rules on the way border controls are carried out or with the EU rules regulating entry and exit from the territory of the Union and co-exist with and leave those rules intact.
- (30) As a result of the legal and technical differences between national provisions concerning the processing of personal data, including PNR, air carriers are and 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. These differences may be prejudicial to effective cooperation between the competent national authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.
- (31) Since the objectives of this Directive cannot be sufficiently achieved by the Member States, and can be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

²¹ NL proposal.

- (32) This Directive respects the fundamental rights and the principles of the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 of the Charter and has to be implemented accordingly. The Directive is compatible with data protection principles and its provisions are in line with the Framework Decision 2008/977/JHA. [Furthermore, and in order to comply with the proportionality principle, the Directive, on specific issues, will have stricter rules on data protection than the Framework Decision 2008/977/JHA]²².
- (33) In particular, the scope of the Directive is as limited as possible, it allows retention of PNR data for period of time not exceeding 5 years²³, after which the data must be deleted, the data must be masked out after a very short period, the collection and use of sensitive data is prohibited. In order to ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority is responsible for advising and monitoring how PNR data are processed. All processing of PNR data must be logged or documented for the purpose of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of the data processing. Member States must also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.
- (34) [In accordance with Article 3 of the Protocol (No 21) on the position of United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, those Member States have notified their wish to participate in the adoption and application of this Directive] OR [Without prejudice to Article 4 of the Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, those Member States will not participate in the adoption of this Directive and will not be bound by or be subject to its application].

²² The necessity of the sentence is being analysed.

²³ ES wishes a less binding wording.

- (35) In accordance with Articles 1 and 2 of the Protocol (No 22) on the position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive provides for the transfer by air carriers of Passenger Name Record data of passengers of extra-EU flights to and from the Member States, as well as the processing of that data.
2. The PNR data collected in accordance with this Directive may be processed only for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime according to Article 4 (2) (a), (b) and (c).²⁴

²⁴ NL demanded that the combating of illegal immigration be added to the scope of the proposal. This was opposed by BE. In line with the suggestion of many delegations, as voiced during the September 30th meeting and forwarded to the Presidency in subsequent written comments, the “transnational” qualification has been deleted.

Article 1a

Application of the directive to intra-EU flights

1. A Member State may give notice in writing to the Commission that it wishes to apply the provisions of this Directive to intra-EU flights. The Commission shall publish such a notice in the Official Journal of the European Union. A Member State may give such notice at any time following the period of two years after the entry into force of this Directive.
2. Where such a notice is given, all the provisions of this Directive shall apply in relation to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if it were PNR data from extra-EU flights.
3. A Member State who applies this Directive to intra-EU flights shall decide the particular intra-EU flights for which it wishes PNR data to be transferred to its national Passenger Information Unit. It shall make this decision by choosing the particular flights it considers necessary in order to further the purposes of this Directive. It may decide to change the particular intra-EU flights at any time. The Member State shall communicate its decision to each affected carrier in accordance with procedures adopted in accordance with Article 14.

Article 2

Definitions

For the purposes of this Directive 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;
- (b) 'extra-EU flight' means any scheduled or non-scheduled flight by an air carrier planned to land on the territory of a Member State originating in a third country or to depart from the territory of a Member State with a final destination in a third country, including in both cases any transfer or transit flights;
- (c) 'intra-EU flight' means any scheduled or non-scheduled flight by an air carrier planned to land on the territory of a Member State originating in another Member State or to depart from the territory of a Member State with a final destination in another Member State, including in both cases any transfer or transit flights
- (d) 'Passenger Name Record' or 'PNR data' means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers²⁵ for each journey booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS) or equivalent systems providing the same functionalities;
- (e) 'passenger' means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the carrier [which is manifested by the persons' registration in the passengers list]²⁶;
- (f) 'reservation systems' means the air carrier's internal reservation system, in which PNR data are collected for the handling of reservations;

²⁵ FR and NL remarked that the exact IATA terminology should be used for "participating air carriers".

²⁶ GR proposal.

- (g) 'push method' means the method whereby air carriers transfer the required PNR data into the database of the authority requesting them;
- (h) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;
- (i) 'serious crime' means the offences under national law referred to in Article 2(2) of Council Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years²⁷ under the national law of a Member State;
- (k) 'masking out of data' means [rendering certain data elements of such data unavailable to a user without deleting these data elements]²⁸.

²⁷ NL would like the period to be 4 years.

²⁸ CZ proposal.

CHAPTER II
RESPONSIBILITIES OF THE MEMBER STATES

Article 3

Passenger Information Unit

1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime or a branch of such an authority to act as its ‘Passenger Information Unit’ responsible for collecting PNR data from the air carriers, storing them, analysing them and transmitting the result of the analysis to the competent authorities referred to in Article 5. Its staff members may be seconded from competent public authorities²⁹.
2. Two or more Member States may establish or designate a single 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 States. The participating Member States shall agree on the detailed rules for the operation of the Passenger Information Unit and shall respect the requirements laid down in this Directive.
3. Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and may at any time update its declaration. The Commission shall publish this information, including any updates, in the *Official Journal of the European Union*.

²⁹ AT reservation on the proposed decentralised architecture.

Article 4

Processing of PNR data

1. The PNR data transferred by the air carriers, pursuant to Article 6, in relation to extra-EU flights, shall be collected by the Passenger Information Unit of the relevant Member State. Should the PNR data transferred by air carriers include data beyond those listed in Annex 1, the Passenger Information Unit shall delete such data immediately upon receipt.
2. The Passenger Information Unit shall process PNR data only³⁰ for the following purposes:
 - (a) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities referred to in Article 5. [In carrying out such an assessment the Passenger Information Unit may compare PNR data against relevant databases].

When the assessment is carried out with regard to terrorist offence or to serious crimes listed in Annex 2, the Passenger Information Unit may process PNR data against pre-determined criteria. Member States shall ensure that any positive match resulting from automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action³¹;

³⁰ FR wishes the word „only” to be deleted.

³¹ DE expressed doubts on the operational added value of pro-active use of PNR data and requested further evidence thereof. Other delegations, however, remarked that the use of risk criteria was meant to reduce the number of controls by arriving at more focused controls.

(b) responding, on a case-by-case basis, to duly reasoned requests from competent authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and to provide the competent authorities with the results of such processing; and

(c) analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify any persons who may be involved in a terrorist offence or serious crimes listed in Annex 2 pursuant to point (a).

3. The assessment of the passengers prior to their scheduled arrival or departure from the Member State carried out against pre-determined criteria referred to in point (a) of paragraph 2 shall be carried out in a non-discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities referred to in Article 5. The assessment criteria shall in no circumstances be based on characteristics enumerated in Article 21 of the Charter of Fundamental Rights³².
4. The Passenger Information Unit of a Member State shall transfer the PNR data or the results of the processing of PNR data of the persons identified in accordance with point (a) of paragraph 2 for further examination to the relevant competent authorities of the same Member State. Such transfers shall only be made on a case-by-case basis.

³² FR and UK suggest that the assessment criteria allowed are: age, sex and nationality. NL wished that the allowed criteria are age and sex.

Article 5

Competent authorities

1. Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of the processing of PNR data from the Passenger Information Units in order to examine that information further or take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.
2. Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.
3. Each Member State shall notify the list of its competent authorities to the Commission twelve months after entry into force of this Directive at the latest, and may at any time update its declaration. The Commission shall publish this information, as well as any updates, in the *Official Journal of the European Union*.
4. The PNR data of passengers and the result of the processing of PNR data received by the Passenger Information Unit may be further processed by the competent authorities of the Member States only³³ for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.
5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing³⁴.

³³ FR wishes the word „only” to be deleted.

³⁴ ES scrutiny reservation.

6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of characteristics enumerated in Article 21 of the Charter of Fundamental Rights.

Article 6

Obligations on air carriers

1. Member States shall adopt the necessary measures to ensure that air carriers transfer ('push') the PNR data as defined in Article 2(c) and specified in the Annex 1, to the extent that such data are already collected by them, to the database of the national Passenger Information Unit of the Member State on the territory of which the extra-EU flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers, the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where the flight has one or more stop-overs at the airports of the Member States, air carriers shall transfer the PNR data to the Passenger Information Units of all the Member States concerned.
2. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the procedure of Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:
 - (a) 24 to 48 hours before the scheduled time for flight departure;and
 - (b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board.

3. Member States may permit air carriers to limit the transfer referred to in point (b) of paragraph 2 to updates of the transfer referred to in point (a) of paragraph 2.
4. On a case-by-case basis, in duly substantiated cases, upon request from a Passenger Information Unit in accordance with national law, air carriers shall transfer PNR data where access earlier than that mentioned in point (a) of paragraph 2 is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime.

Article 7³⁵

Exchange of information between Member States³⁶

1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2)(a), the PNR data or the result of the processing of PNR data is transmitted by that Passenger Information Unit to the Passenger Information Units of other Member States where the former Passenger Information Unit considers such transfer to be necessary for the prevention, detection, investigation or prosecution of terrorist offences, or serious crime³⁷. The Passenger Information Units of the receiving Member States shall transmit such PNR data or the result of the processing of PNR data to their relevant competent authorities. The latter transfers shall only be made on a case-by-case basis.

³⁵ FR wishes the purpose of this Article to be to make possible the exchange of PNR data or their analysis between Member States in a supervised way and taking account of the feasibility of the proposed arrangements.

³⁶ NL scrutiny reservation. DE, NL and SI thought that the proposed drafting was not detailed enough and left too much vagueness as to how data should be transferred. UK indicated it was concerned about sharing of the results of processing that might divulge intelligence sources. COM reassured this was not intended by this proposed text.

³⁷ AT proposed to limit this to "the prevention of an immediate and serious threat to public security".

2. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(1), and, if necessary, also the result of the processing of PNR data. The duly reasoned request for such data may be based on any one or a combination of data elements, as deemed necessary by the requesting Passenger Information Unit for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime. Passenger Information Units shall provide the requested data as soon as practicable and shall provide also the result of the processing of PNR data, if it has already been prepared pursuant to Article 4(2)(a) ³⁸.

3. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(2), and, if necessary, also the result of the processing of PNR data. The Passenger Information Unit may make a duly reasoned request access to specific PNR data kept by the Passenger Information Unit of another Member State in their full form without the masking out only in exceptional circumstances³⁹ in response to a specific threat or a specific investigation or prosecution related to terrorist offences or serious crime.

³⁸ FR and SI thought that this provision should be more fleshed out. DE thought that possibility for the requested Member States to check the request, in particular against the necessity requirement, should be stipulated here. COM thought that only the requesting Member State should assess the necessity requirement.

³⁹ FR requested clarification as to what was covered by this term and that it is the requesting PIU who should assess the exceptional circumstances.

4. Only in those cases where it is necessary for the prevention of an immediate and serious threat to public security may the competent authorities of a Member State request directly the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(1) and (2). Such requests, a copy of which shall always be sent to the Passenger Information Unit of the requesting Member State, shall relate to a specific investigation or prosecution of terrorist offences or serious crime and shall be reasoned, in particular as regards the immediate and serious nature of the threat. Passenger Information Units shall respond to such requests as a matter of priority. In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.
5. Exceptionally, where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the Passenger Information Unit of a Member State shall have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights landing in or departing from the latter's territory at any time.
6. Exchange of information under this Article may take place using any existing channels for international law enforcement cooperation^{40 41}. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contacts to which requests may be sent in cases of urgency. The Commission shall communicate to the Member States and the Committee set up in accordance with Article 14 (1) the notifications received.

⁴⁰ AT proposed to replace this sentence with the following text: "To effectively guarantee the legality of information exchange under this Article Member States shall provide for adequate mechanisms of control by the independent supervisory authority(ies) pursuant to Article 12. An exchange of information according to para 2 to 5 of this Article may only take place upon duly motivated request on a case by case basis. Direct access shall be excluded." The Presidency thinks that these proposed additions are superfluous in that they already flow from the previous paragraphs. As to the role of the supervision authorities, this should be regulated under Article 12.

⁴¹ BE asked whether security services could be designated as competent authorities and whether these would be allowed to use their own, dedicated channels for exchange of information.

Article 8

Transfer of data to third countries⁴²

A Member State may transfer PNR data stored in accordance with Article 9 and the results of the processing of PNR data stored by the Passenger Information Unit data to a third country, only on a case-by-case basis and if:

- (a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled,
- (b) the transfer is necessary for the purposes of this Directive specified in Article 1(2),
- (c) the third country agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive specified in Article 1(2) and only with the express authorisation of the Member State; and
- (d) similar conditions as those laid down in Article 7(2), (3) or (4) are fulfilled.

⁴² DE and LV thought the requirement for prior consent of the originating Member State should be clarified.

Period of data retention

1. Member States shall ensure that the PNR data provided by the air carriers to the Passenger Information Unit are retained in a database at the Passenger Information Unit for a period of

⁴³ NL propose new draft of the Article 9 as follows:

1. For the purposes mentioned in articles 4(2)(a), 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 [...] days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.

2. The result of the matching referred to in paragraph 1, shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities of a positive match.

3. For the purposes mentioned in articles 4(2)(b) and 4(2)(c), 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 [...] years after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.

- a) For the purpose of article 4(2)(b), access to the PNR data shall be permitted only by the Head of the Passenger Information Unit or by judicial authority designated by the Member State and only where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution.

- b) For the purpose of article 4(2)(c), the PNR data shall be masked out and shall be accessible only to personnel specifically authorised to carry out an analysis of PNR data and develop assessment criteria according to article 4(2)(c). For the purpose of this Directive, the data elements which could serve to identify the passenger to whom PNR data relate and which should be filtered and masked out are at least the following: - Name(s), including the names of other passengers on PNR and number of travellers on PNR travelling together;

- Address and contact information;

- All forms of payment information, including billing address;

- Complete travel itinerary for specific PNR;

- Frequent flyer information;

- General remarks to the extent that it contains any information which could serve to identify the passenger to whom the PNR relate; and

- Any collected Advance Passenger Information.

4. 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 specified in paragraph 3. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.

30 days⁴⁴ after their transfer to the Passenger Information Unit of the first Member State on whose territory the extra-EU flight is landing or departing⁴⁵.

2. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be retained at the Passenger Information Unit for a further period of five years. During this period, all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such masked out PNR data shall be accessible only to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria according to Article 4(2)(c). Access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit or by judicial authority designated by the Member State for the purposes of Article 4(2)(b) and where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution⁴⁶.

For the purposes of this Directive, all data elements which could serve to identify the passenger to whom PNR data relate and which should be filtered and masked out are in particular the following:

1. Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together;
2. Address and contact information;
3. All forms of payment information, including billing address;
4. Complete travel itinerary for specific PNR;

⁴⁴ FR opts for 1 year, in case simultaneous shortening of the period mentioned in para 2 to 4 years.

⁴⁵ DE requested which types of processing would be possible during this 30 days period, in addition to the types of processing allowed during the second, five year, period.

⁴⁶ Some Member States thought that it should be left to each individual Member State to decide who could access the full PNR data under those circumstances (CZ, EE, LV) or that the proposed system was too complex (FR). Other Member States were of the opinion that additional guarantees should be provided for this access to full PNR data: AT, DE, BE and NL.

5. Frequent flyer information;
 6. General remarks to the extent that it contains any information which could serve to identify the passenger to whom PNR relate; and
 7. Any collected Advance Passenger Information.
3. Member States shall ensure that the PNR data are deleted upon expiry of the period specified in paragraph 2. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.
 4. The result of matching referred to in Article 4(2)(a) shall be kept by the Passenger Information Unit 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 individual review by non-automated means, proven to be negative, it shall, however, be stored so as to avoid future 'false' positive matches for a maximum period of three years unless the underlying data have not yet been deleted in accordance with paragraph 3 at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.

Article 10

Penalties against air carriers

Member States shall ensure, in conformity with their national law, that dissuasive, effective and proportionate penalties, including financial penalties, are provided for against air carriers which, do not transmit the data required under this Directive, to the extent that they are already collected by the them, or do not do so in the required format or otherwise infringe the national provisions adopted pursuant to this Directive.

Article 11

Protection of personal data

1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as those adopted under national law in implementation of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA. The provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable.
2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of the Council Framework Decision 2008/977/JHA regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.
3. Any processing of PNR data based on characteristics enumerated in Article 21 of the Charter of Fundamental Rights shall be prohibited. In the event that PNR data revealing such information are received by Passenger Information Unit they shall be deleted immediately.
4. All processing, including receipt of PNR data from air carriers and all transfer of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States and third countries, even if refused, shall be logged or documented by the Passenger Information Unit and the competent authorities for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of data processing, in particular by the national data protection supervisory authorities. These logs shall be kept for a period of five years unless the underlying data have not yet been deleted in accordance with Article 9(3) at the expiry of those five years, in which case the logs shall be kept until the underlying data are deleted.

5. Member States shall ensure that air carriers, their agents or other ticket sellers for the carriage of passengers on air service inform passengers of extra-EU flights at the time of booking a flight and at the time of purchase of a ticket in a clear and precise manner 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, the possibility of exchanging and sharing such data and their data protection rights, in particular the right to complain to a national data protection supervisory authority of their choice⁴⁷. The same information shall be made available by the Member States to the public⁴⁸.
6. Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited⁴⁹.

Article 12

National supervisory authority

Each Member State shall provide that the national supervisory authority or authorities established in implementation of Article 25 of Framework Decision 2008/977/JHA shall also be responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to the present Directive. The further provisions of Article 25 Framework Decision 2008/977/JHA shall be applicable.

⁴⁷ DE, EE and FR queried how the European Union could impose such obligation on third countries from which air carriers fly to Member States.

⁴⁸ FR expressed a preference for system, like the one regarding SIS, whereby passengers are informed at the airports.

⁴⁹ CZ, EE and NL were opposed to such blanket ban, whereas SI supported it. COM stated that, in its view, this paragraph did not prevent Members from sharing information with private companies that worked with the government.

CHAPTER IV

IMPLEMENTING MEASURES

Article 13

Common protocols and supported data formats

1. All transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made by electronic means or, in the event of technical failure, by any other appropriate means, for a period of one year following the adoption of the common protocols and supported data formats in accordance with Article 14.
2. Once the period of one year from the date of adoption of the common protocols and supported data formats has elapsed, all transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.
3. The list of accepted common protocols and supported data formats shall be drawn up and, if need be, adjusted, by the Commission in accordance with the procedure referred to in Article 14(2).
4. As long as the accepted common protocols and supported data formats referred to in paragraphs 2 and 3 are not available, paragraph 1 shall remain applicable.
5. Each Member State shall ensure that the necessary technical measures are adopted to be able to use the common protocols and data formats within one year from the date the common protocols and supported data formats are adopted.

Article 14

Committee procedure

1. The Commission shall be assisted by a committee ('the Committee'). That Committee shall be a committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers shall apply.

CHAPTER V

FINAL PROVISIONS

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest 36 months after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions.

When Member States adopt those provisions, they shall contain a reference to this Directive 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. [Without prejudice to Article 10, Member States shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Directive]⁵⁰.
3. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

[Article 16

Costs⁵¹

1. The costs of setting up Passenger Information Units shall be subsidised from the general budget of the European Union (Commission section).
2. Each Member State shall bear the costs of operation of the relevant Passenger Information Unit.
3. Air carriers shall bear the costs arising from the administration, use and maintenance of the software referred to in Article 13.]

Article 17

Review

1. The Committee set up in accordance with Article 14 (1) shall be convened regularly at least [twice] a year in order to share experiences and discuss relevant issues within the scope and subject matter of the Directive.⁵²

⁵⁰ Sentence copied from previous paragraph 7 of Article 12.

⁵¹ The Commission expressed strong reservation to the inclusion of this provision in the text of the directive.

⁵² As there might be legal obstacles for the Committee to assume the proposed tasks, a different organisational structure, i.e. an expert group is to be considered with this regard.

2. On the basis of the Committee's deliberations as well as other information provided by the Member States the Commission shall undertake a review of the operation of this Directive and submit a report to the European Parliament and the Council within four years after the date mentioned in Article 15(1).

Such review shall cover all the elements of this Directive. It shall also contain the statistical information referred to in Article 18 (4).

3. On the basis of the report mentioned in paragraph 2 and in line with the experiences gained by the Member States, the Commission shall consider the necessity of putting forward amendments to this Directive.

Article 18

Statistical data

1. Member States shall provide the Commission with a set of statistical information on PNR data provided to the Passenger Information Units. These statistics shall not contain any personal data.
2. The statistics shall as a minimum cover:
 1. total number of persons whose PNR data were collected and exchanged;
 2. number of persons identified for further scrutiny;
 3. number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination;

3. The Commission acting in accordance with the procedure referred to in Article 14(2) may widen the scope of collected statistics if that proves necessary⁵³.
4. On a yearly basis, the Commission shall provide the Council with cumulative statistics referred to in Article 18 (1).

Article 19

Relationship to other instruments

1. Member States may continue to apply bilateral or multilateral agreements or arrangements between themselves on exchange of information between competent authorities, in force when this Directive is adopted, in so far as such agreements or arrangements are compatible with this Directive.
2. This Directive is without prejudice to any obligations and commitments of Member States or of the Union by virtue of bilateral and/or multilateral agreements with third countries.

Article 20

Entry into force

This Directive shall enter into force the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament

The President

For the Council

The President

1. ⁵³ EE and UK pointed out that the exact requirements for statistics need to be known in advance as there could be difficulty in retrieving statistics retrospectively.

Passenger Name Record data as far as collected by air carriers

- (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) Complete 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 Advance Passenger Information (API) data collected
- (19) All historical changes to the PNR listed in numbers 1 to 18

1. participation in a criminal organisation.
 2. trafficking in human beings.
 3. sexual exploitation of children and child pornography.
 4. illicit trafficking in narcotic drugs and psychotropic substances.
 5. illicit trafficking in weapons, munitions and explosives.
 6. laundering of the proceeds of crime.
 7. illicit trade in human organs and tissue
 8. facilitation of unauthorised entry and residence
 9. kidnapping, illegal restraint and hostage-taking.
 10. illicit trafficking in cultural goods, including antiques and works of art
 11. illicit trafficking in nuclear or radioactive materials
 12. unlawful seizure of aircraft
 13. sabotage
-