



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 23 April 2012**

**8916/12**

---

---

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

---

---

**GENVAL 23  
AVIATION 73  
DATAPROTECT 52  
CODEC 1024**

**NOTE**

---

from: Presidency  
to: Council

---

No. prev. doc.: 8448/1/12 REV 1 GENVAL 17 AVIATION 60 DATAPROTECT 40  
CODEC 897

---

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

---

**Background**

1. The Commission submitted the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes to the Council on 17 November 2007. This proposal was discussed in detail during the Slovenian, the French and the Czech Presidency. When the Lisbon Treaty entered into force, the proposal, which was not yet adopted, became legally obsolete.
2. On 3 February 2011 the Commission presented a proposal for a 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.

3. At the Council meeting on 11 April 2011, a discussion was held on whether intra-EU flights should be included in the scope of the draft Directive. Further to that discussion, the preparatory work on the draft PNR Directive continued at expert-level at the Working Party on General Matters, including Evaluations on the basis of the indication by the Council that the Directive should allow individual Member States the option to mandate the collection of PNR data with regard to intra-EU flights and that the collection and processing of such data should be subject to the legal regime created by the PNR Directive<sup>1</sup>.
4. Since the Commission presented its proposal, the Working Party on General Matters, including Evaluations has worked on the proposal for over a year. The scope of the proposal has been thoroughly discussed and further refined and it is now established for which purposes and under which conditions PNR data collected under the Directive can be used. A few Member States have argued in favour of extending the scope of the Directive to other purposes than those presently covered. It is, however, the Presidency's assessment that a clear and strict purpose limitation is important in order to safeguard the proportionality of the Directive. The Presidency therefore considers that no further changes should be made to the scope of the Directive at the present stage. The review clause in the proposal will, however, allow for future revision of the Directive on the basis of national experiences.
5. The Presidency considers that the extensive work on the file and the considerable efforts that have been made to take all views into account during the Hungarian, Polish and Danish Presidency have resulted in a well-balanced draft Directive.
6. Nine delegations maintain a general scrutiny reservation on the proposal, two have a general reservation and two hold a parliamentary scrutiny reservation.

---

<sup>1</sup> 9103/11 GENVAL 43 AVIATION 100 DATAPROTECT 34 CODEC 648.

## **Retention period**

7. The Commission had proposed an initial storage period of 30 days, followed by a further retention period of five years of masked out data. The negotiations have shown that an initial storage period of 30 days is generally considered much too short from an operational point of view. Article 9 has been redrafted in such a way that the overall retention period of 5 years is subdivided into two periods: a first period in which the data are fully accessible and a second period during which the data are masked out and where full disclosure of the data is subject to strict conditions. Taking into consideration the operational needs the initial retention period is set at two years. In comparison the initial retention period in the 2011 EU-Australia Agreement, to which the Council has agreed and the EP has given its consent, is three years.

### **Inclusion of intra-EU flights**

8. Article 1a, which has been drafted in line with the indications given at the Council meeting on 11 April 2011, allows Member States to apply this Directive to all or selected intra-EU flights. Hence, the Article allows any Member State to collect PNR data from those intra-EU flights it considers necessary in order to prevent, detect, investigate or prosecute serious crime or terrorism. It thus constitutes a compromise between those Member States that are in favour of mandatory inclusion of all intra-EU flights and those that are opposed to any inclusion of intra-EU flights.
9. The Presidency considers the above solutions as part of a package, which constitutes a compromise between those Member States which would prefer to limit the impact of the collection and processing of PNR data and those Member States which are in favour of an extension of the scope of the collection and processing of PNR data. At the Coreper meeting of 18 April 2012 some Member States maintained for the time being their reservations on the issues of retention periods and intra-EU flights. However, only three delegations indicated that they could not accept the overall package as a basis for commencing negotiations with the EP.
10. *In view of the above, the Presidency invites the Council to confirm the compromise text set out in the Annex as a basis for starting the negotiations with the Parliament.*

**DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on the use of Passenger Name Record (PNR) 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 European Commission,

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

Having regard to the opinion of the European Economic and Social Committee<sup>2</sup>,

Having regard to the opinion of the Committee of the Regions<sup>3</sup>,

Acting in accordance with the ordinary legislative procedure,

---

<sup>2</sup> OJ C , , p. .

<sup>3</sup> 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 purposes. 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'<sup>4</sup> 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" 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 data<sup>5</sup> regulates the transfer of advance passenger data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration.
- (5) PNR data are necessary to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, inter alia 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.
- (6)

---

<sup>4</sup> 17024/09 CO EUR-PREP 3 JAI 896 POLGEN 229.

<sup>5</sup> OJ L 261, 6.8.2004, p. 24.

- (7) PNR data enable to identify persons who were previously "unknown", i.e. persons previously unsuspected of involvement in terrorism or serious crime, 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 it is possible to address the threat of terrorism and serious crime 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. Furthermore, the assessment criteria shall be defined in a manner which ensures that as few innocent people as possible are identified by the system.
- (8) 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.
- (9) Some air carriers retain any collected advance passenger information (API) data as part of the PNR data, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual and thus reinforcing their law enforcement value and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that, where air carriers collect API data, they should transfer it, irrespective of whether the API data is retained as part of the PNR data or not.
- (10) In order 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 extra EU-flights, and if the Member State wishes to do so also on air carriers operating intra EU-flights, to transfer any collected PNR and API data. These provisions should be without prejudice to Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

- (11) The processing of personal data must be proportionate to the specific security goals pursued by this Directive.
- (12) The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA on combating terrorism<sup>6</sup> and the definition of serious crime applied in this Directive should be the same as in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedure between Member States<sup>7</sup>. The list of relevant serious crime with relation to which PNR data may be used for the creation and application of assessment criteria should be based on Framework Decision 2002/584/JHA.
- (13) PNR data should be transmitted to a single designated unit (Passenger Information Unit) in the relevant Member State, so as to ensure clarity and reduce costs to air carriers. The Passenger Information Unit may have different locations in one Member State and Member States may also jointly set up one Passenger Information Unit.
- (13a) It is desirable that co-financing of the costs related to the establishment of the national Passenger Information Units will be provided for under the instrument for financial support for police cooperation, preventing and combating crime, and crisis management as part of the Internal Security Fund.
- (14) The contents of any lists of required PNR data to be obtained by a 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 a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life. 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.

---

<sup>6</sup> OJ L 164, 22.6.2002, p. 3.

<sup>7</sup> 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 provided for 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 powers<sup>8</sup>.
- (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 and serious crime.
- (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, in respect of Article 21 of the Charter of Fundamental Rights of the European Union no such decision should discriminate on any grounds such as a person’s sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

---

<sup>8</sup> OJ L 55, 28.02.2011, p. 13.



- (20) Member States should share with other Member States the PNR data that they receive where this 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)<sup>9</sup> 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 Union<sup>10</sup>. Such exchange of PNR data between law enforcement 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 depersonalised through masking out and that the full PNR data are only accessible under very strict and limited conditions.
- (22) Where specific PNR data have been transmitted 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 out in 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 matters<sup>11</sup>.

---

<sup>9</sup> OJ L 121, 15.5.2009, p. 37.

<sup>10</sup> OJ L 386, 29.12.2006, p. 89.

<sup>11</sup> OJ L 350, 30.12.2008, p. 60.

- (24) Taking into consideration the right to the protection of personal data, the rights of the data subjects concerning the 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.
- (25a) This Directive allows the principle of public access to official documents to be taken into account.
- (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 requirements relating to the purpose and the necessity of the transfer.
- (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 of the provisions adopted by the Member States pursuant to 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) This Directive is without prejudice to the current Union rules on the way border controls are carried out or with the Union rules regulating entry and exit from the territory of the Union.

- (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.
- (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 thereof 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.
- (33) In particular, the scope of this Directive is as limited as possible, as it allows retention of PNR data in the Passenger Information Units for period of time not exceeding 5 years, after which the data should be deleted, as the data should be depersonalised through masking out after an initial period, and as 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 the way PNR data are processed. All processing of PNR data should be logged or documented for the purpose of verification of its legality, self-monitoring and ensuring proper data integrity and security of the processing. Member States should 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.
- (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 (PNR) 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 as provided for in Article 4 (2) (a), (b) and (c).

## *Article 1a*

### **Application of the directive to intra-EU flights**

1. If a Member State wishes to apply this Directive to intra-EU flights, it shall give notice in writing to the Commission to that end. The Commission shall publish such a notice in the *Official Journal of the European Union*. A Member State may give or revoke such notice at any time 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 may decide to apply this Directive only to selected intra-EU flights. In making such a decision the Member State shall select the flights it considers necessary in order to further the purposes of this Directive. The Member State may decide to change the selected intra-EU flights at any time.

## *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 flying from a third country planned to land on the territory of a Member State or from the territory of a Member State planned to land in a third country, including in both cases flights with any stop-overs at the territory of Member States or third countries;
- (c) ‘intra-EU flight’ means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State planned to land on the territory of one or more of the other Member States, without any stop-overs at the territory/airports of a third country;

- (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 carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS, the system used to check passengers onto flights) 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 air carrier, which is manifested by the persons' registration in the passengers list and which includes transfer or transit passengers;
- (f) 'reservation systems' means the air carrier's internal reservation system, in which PNR data are collected for the handling of reservations;
- (g) 'push method' means the method whereby air carriers transfer 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 years under the national law of a Member State;
- (k) 'depersonalising through masking out of data' means rendering certain data elements of such data invisible to a user without deleting these data elements.

## 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' ("PIU") responsible for collecting PNR data from the air carriers, storing them, processing them and transmitting the PNR data or the result of the processing thereof to the competent authorities referred to in Article 5. The PIU is also responsible for the exchange of PNR data or the result of the processing thereof with PIUs of other Member States in accordance with Article 7. Its staff members may be seconded from competent public authorities. It shall be provided with adequate resources in order to fulfil its tasks.
2. Two or more Member States may establish or designate a single authority to serve as their Passenger Information Unit. Such a 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 within one month of the establishment or designation of the Passenger Information Unit thereof. It may at any time modify its notification. The Commission shall publish this information, including any modifications of it, in the *Official Journal of the European Union*.

## Article 4

### Processing of PNR data

1. The PNR data transferred by the air carriers shall be collected by the Passenger Information Unit of the relevant Member State, as provided for in Article 6. Should the PNR data transferred by air carriers include data beyond those listed in Annex I, the Passenger Information Unit shall delete such data immediately upon receipt.
2. The Passenger Information Unit shall process PNR data only for the following purposes:
  - (a) carrying out an assessment of the passengers prior to their scheduled arrival to or departure from the Member State in order to identify persons who require further examination by the competent authorities referred to in Article 5, in view of the fact that such persons may be involved in a terrorist offence or serious crime.
    - (i) In carrying out such an assessment the Passenger Information Unit may compare PNR data against databases relevant for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases.
    - (ii) When carrying out an assessment of persons who may be involved in a terrorist offence or serious crime listed in Annex II to this Directive, the Passenger Information Unit may also process PNR data against pre-determined criteria.

Member States shall ensure that any positive match resulting from automated processing of PNR data conducted under point (a) of paragraph 2 is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action in accordance with national law;

(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 referred to point (a) (ii) in order to identify any persons who may be involved in a terrorist offence or serious crimes listed in Annex II.

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)(ii) 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 a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life.
4. The Passenger Information Unit of a Member State shall transmit 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 competent authorities of the same Member State referred to in Article 5. Such transfers shall only be made on a case-by-case basis.
5. The consequences of the assessments of passengers referred to in point (a) of paragraph 2 shall not jeopardise the right of entry of persons enjoying the Union right of free movement into the territory of the Member State concerned as laid down in Directive 2004/38/EC. In addition, the consequences of such assessments, where these are carried out in relation to intra-EU flights between Member States to which the Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders<sup>12</sup> applies, shall comply with that Code.

---

<sup>12</sup> OJ L 105, 13.4.2006, p. 1.

## 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. The authorities referred to in paragraph 1 shall be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.
3. For the purpose of Article 7(4), each Member State shall notify the list of its competent authorities to the Commission eighteen months after entry into force of this Directive at the latest, and may at any time update this notification. The Commission shall publish this information, as well as any modifications of it, in the *Official Journal of the European Union*.
4. The PNR data and the result of the processing of PNR data received from the Passenger Information Unit may be further processed by the competent authorities of the Member States only 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 violations of criminal law, or indications thereof, are detected in the course of enforcement action further to such processing.
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.

## Article 6

### Obligations on air carriers on transfer of data

1. Member States shall adopt the necessary measures to ensure that air carriers transfer ('push') the PNR data as defined in Article 2(d) and specified in Annex I, to the extent that such data are already collected by them, to the database of the Passenger Information Unit of the Member State on the territory of which the flight will land and/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 an extra-EU flight has one or more stopovers at the airports of different Member States, air carriers shall transfer the PNR data of all passengers to the Passenger Information Units of all the Member States concerned. This also applies where an intra-EU flight has one or more stopovers at the airports of different Member States, but only in relation to Member States which are collecting PNR data.
  - 1a. In case the air carriers have collected any advance passenger information (API) data listed under item (18) of Annex 1 to this directive but do not retain these data as part of the PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer ('push') these data to the Passenger Information Unit of the Member State referred to in paragraph 1. In case of such transfer, all the provisions of this Directive shall apply in relation to these API data as if they were part of the PNR data.
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 referred to in Articles 13 and 14, or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:
  - (a) once 24 to 48 hours before the scheduled time for flight departure;and
  - (b) once immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.

3. Member States shall 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 and where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, air carriers shall, upon request from a Passenger Information Unit in accordance with the procedures provided under national law, transfer PNR data at other points in time than those mentioned in paragraph 2(a) and (b).

### *Article 7*

#### **Exchange of information between Member States**

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 any processing thereof is transmitted by that Passenger Information Unit to the corresponding units of other Member States where it considers such transfer to be necessary for the prevention, detection, investigation or prosecution of terrorist offences, or serious crime. The Passenger Information Units of the receiving Member States shall transmit the received information to their competent authorities in accordance with Article 4(4).
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 and have not yet been depersonalised through masking out under Article 9(2) and, if necessary, also the result of any processing thereof, if it has already been prepared pursuant to Article 4(2)(a). 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. In case the requested data have been depersonalised through masking out in accordance with Article 9(2) the Passenger Information Unit shall only provide the full PNR data where it is reasonably believed that it is necessary for the purpose of Article 4(2)(b) and only when authorised to do so by an authority competent under Article 9(3).

3. (...)
4. Only when necessary in cases of emergency and under the conditions laid down in paragraph 2 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. The requests from the competent authorities, a copy of which shall always be sent to the Passenger Information Unit of the requesting Member State, shall be reasoned. In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.
5. Exceptionally, where access to PNR data 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 at any time have the right to request the Passenger Information Unit of another Member State to obtain PNR data in accordance with article 6(4) and provide it to the requesting Passenger Information Unit.
6. Exchange of information under this Article may take place using any existing channels for cooperation between the competent authorities of the Member States. 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 contact points to which requests may be sent in cases of emergency. The Commission shall communicate to the Member States the notifications received.

## *Article 8*

### **Transfer of data to third States**

A Member State may transfer PNR data as well as the results of the processing of such data stored by the Passenger Information Unit in accordance with Article 9 to a third State 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) it is necessary for the purposes of this Directive as specified in Article 1(2);
- (c) the third State agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive as specified in Article 1(2) and only with the express authorisation of the Member State that provided the third State with the data; and
- (d) similar conditions as those laid down in Article 7(2) are fulfilled.

## *Article 9*

### **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 five years after their transmission to the Passenger Information Unit of the Member State on whose territory the flight is landing or departing.

2. Upon expiry of a period of two years after the transfer of the PNR data as referred to in paragraph 1, the PNR data shall be depersonalised through masking out of the following data elements which could serve to directly identify the passenger to whom the PNR data relate:
  1. Name (s), including the names of other passengers on PNR travelling together;
  2. Address and contact information;
  3. All forms of payment information, including billing address, to the extent that it contains any information which could serve to directly identify the passenger to whom PNR relate or any other persons;
  4. Frequent flyer information;
  5. General remarks to the extent that it contains any information which could serve to directly identify the passenger to whom the PNR relate; and
  6. Any collected advance passenger information.
3. Upon expiry of the two-year period referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is reasonably believed that it is necessary for the purpose of Article 4(2)(b) and only when approved by a judicial authority or by another national authority competent under national law to verify whether the conditions for disclosure are fulfilled.
4. Member States shall ensure that the PNR data are deleted upon expiry of the period specified in paragraph 1. 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 case for the purpose of prevention, detection, investigation or prosecution, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.

5. The result of the processing 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 processing has, further to individual review by non-automated means as referred to in Article 4(2)(a) last subparagraph, proven to be negative, it may, however, be stored so as to avoid future ‘false’ positive matches for as long as the underlying data have not yet been deleted in accordance with paragraph 1.

#### *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 as provided for in Article 6, 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 the national law implementing 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 the national law to implement 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 revealing a person's racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, health or sexual life shall be prohibited. In the event that PNR data revealing such information are received by Passenger Information Unit they shall be deleted without delay.
4. All processing, including receipt of PNR data from air carriers and all transfers 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 concerned 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(4) 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 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 transmission 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 the competent national data protection supervisory authority. The same information shall be made available by the Member States to the public.
6. 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.

## *Article 12*

### **National supervisory authority**

Each Member State shall provide that the national supervisory authority or authorities established to implement 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.

## **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, for the first time, of the common protocols and supported data formats by the Commission in accordance with paragraph 3, 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 those 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 taking due account of ICAO regulations and, if need be, adjusted, by the Commission by means of implementing acts 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 referred to in paragraph 2.

#### *Article 14*

#### **Committee procedure**

1. The Commission shall be assisted by a 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. The Commission shall not adopt the draft implementing act when no opinion is delivered by the Committee and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 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. 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 17*

#### **Review**

1. The Council shall, at the appropriate level, discuss regularly the practical experiences and relevant issues within the scope and subject matter of the Directive.
2. On the basis of these discussions as well as other information provided by the Member States, including the statistical information referred to in Article 18 (2), the Commission shall undertake a review of the operation of this Directive and:

(a) within two years after the date mentioned in Article 15(1) submit a report to the European Parliament and the Council on the feasibility and necessity of including all or selected intra-EU flights in the scope of this Directive on a mandatory basis, taking into account the experience gained by Member States, especially those Member States that in accordance with Article 1a collect PNR with regard to intra-EU flights,

(b) within four years after the date mentioned in Article 15(1) submit a report to the European Parliament and the Council on all other elements of this Directive and on the feasibility and necessity of including transportation providers other than air carriers in the scope of this Directive, taking into account the experience gained by Member States, especially those Member States that collect PNR from other transportation providers.

3. If appropriate, in light of the review referred to in paragraph 2, the Commission shall make a legislative proposal to the European Parliament and the Council with a view to amending this Directive.

### *Article 18*

#### **Statistical data**

1. Member States shall provide on a yearly basis 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 passengers whose PNR data were collected and exchanged;
  2. number of passengers identified for further scrutiny;
  3. number of subsequent law enforcement actions that were taken involving the use of PNR data;

3. 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

For the Council

The President

The President

\_\_\_\_\_

**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 (inter alia document type, document number, nationality, country of issuance, date of document expiration, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time, arrival time)
  - (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. fraud,
7. laundering of the proceeds of crime,
8. computer-related crime,
9. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
10. facilitation of unauthorised entry and residence,
11. illicit trade in human organs and tissue,
12. kidnapping, illegal restraint and hostage-taking,
13. organised and armed robbery,
14. illicit trafficking in cultural goods, including antiques and works of art,
15. forgery of administrative documents and trafficking therein,
16. illicit trafficking in hormonal substances and other growth promoters,
17. illicit trafficking in nuclear or radioactive materials,

18. unlawful seizure of aircraft/ships,

19. sabotage, and

20. trafficking in stolen vehicles.

---