



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 29 April 2011

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

8458/11

LIMITE

**GENVAL 33
AVIATION 78
DATAPROTECT 26
CODEC 545**

PROPOSAL

from: Presidency
to: Working Party on General Matters, including Evaluations
prev.doc. 6007/11 GENVAL 5 AVIATION 15 DATAPROTECT 6 CODEC 278
on: 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) of 8-9 and 28 March 2011, delegations find attached a revised version of the proposed PNR Directive.

As the recitals have not yet been discussed, the Presidency has not made any modifications to the preamble.

The following delegations entered a general scrutiny reservation on the proposal: BE, CZ, ES, FR, GR, IE, LT, LU, NL, PL, and UK.

The following delegations entered 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 purposes¹. 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'² 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'³ 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 data⁴ 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 immigration.
- (5) PNR data are necessary to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security.
- (6) PNR data help law enforcement authorities prevent, detect, investigate and prosecute serious crimes, including acts of terrorism, 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.

¹ COM(2007) 654.

² Council document 17024/09, 2.12.2009.

³ COM(2010) 492.

⁴ OJ L 261, 6.8.2004, p. 24.

- (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 serious crimes that are also transnational in nature, i.e. are intrinsically linked to travelling and hence the type of the data being processed.
- (8) The processing of personal data must be proportionate to the specific security goal pursued by this Directive.
- (9) The use of PNR data together with Advance Passenger Information data in certain cases has added value in assisting Member States in verifying the identity of an individual and thus reinforcing their law enforcement value.
- (10) 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 international flights to or from the territory of the Member States of the European Union.
- (11) 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.

- (12) The definition of terrorist offences should be taken from Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism¹. 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 States². However, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality. The definition of serious transnational crime should be taken from Article 2 of Council Framework Decision 2002/584/JHA and the United Nations Convention on Transnational Organised Crime.
- (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 citizens, notably privacy and the protection of personal data. Such lists should not contain any personal data that could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual life of the individual concerned. 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.

¹ 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).

² 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 advisory procedure foreseen in Regulation (EU) No..... of the European Parliament and the Council [.....]
- (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. Where there are repeated serious infringements which might undermine the basic objectives of this Directive, these penalties may include, in exceptional cases, measures such as the immobilisation, seizure and confiscation of the means of transport, or the temporary suspension or withdrawal of the operating licence.
- (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, no such decision should be taken by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.
- (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)¹ 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 Union². 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 masked out and only accessible under very strict and limited conditions.

¹ OJ L 121, 15.5.2009, p. 37.

² OJ L 386, 29.12.2006, p. 89.

- (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 matters¹ ('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 requirements 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.

¹ OJ L 350, 30.12.2008, p. 60.

- (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, regarding internal flights subject to compliance with relevant data protection provisions, provided that such domestic law respects the Union acquis. The issue of the collection of PNR data on internal flights should be the subject of specific reflection at a future date.
- (29) 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.
- (30) 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.

- (31) 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.
- (32) 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 years, 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.
- (33) [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].

- (34) 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 international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by the Member States and its exchange between them.
2. The PNR data collected in accordance with this Directive may be processed only for the following purposes:
 - (a) The prevention, detection, investigation and prosecution of terrorist offences and serious crime according to Article 4(2)(b) and (c); and

- (b) The prevention, detection, investigation and prosecution of terrorist offences and serious transnational crime according to Article 4(2)(a) and (d)¹.

Article 1a²

Application of the directive to internal flights

1. A Member State may give notice in writing to the Commission that it wishes to apply the provisions of this Directive to internal 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 internal flights as if they were international flights and to PNR data from internal flights as if it were PNR data from international flights.
3. A Member State who applies this Directive to internal flights shall decide the particular internal 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 internal 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.

¹ NL demanded that the combating of illegal immigration be added to the scope of the proposal. This was opposed by BE. Several delegations entered a scrutiny reservation the "transnational" qualification regarding serious crime: AT, BE, CZ, ES, FR, IT, MT, PT, UK.

² Further to the outcome of the Council discussion on 11 April 2011, the Presidency has inserted this proposed new Article on internal flights, on the understanding that this will obviously need to be further discussed. Reservation by AT, DE, LU, SI and MT.

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 passengers¹;
- (b) 'international 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 flights²;
- (bb) 'internal flight' means any scheduled or non-scheduled flight by an air carrier (i) planned to land on the territory of a Member State which has given a notice under article 6A, having originated in another Member State; (ii) planned to depart from the territory of a Member State which has given a notice under article 6A with a final destination in another Member State; including in both cases any transfer or transit flights³
- (c) '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 carriers⁴ 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;

¹ COM clarified that this definition covered charter flights, but excluded air freight companies. EE remarked it did not collect PNR data on charter flights.

² FR requested to clarify what is covered by "transfer" or "transit" flights. COM acknowledged that these terms might not be appropriate, but explained that the purpose was to cover all flight segments of international flights.

³ Further to the outcome of the Council discussion on 11 April 2011, the Presidency has inserted this proposed definition on internal flights, on the understanding that this will obviously need to be further discussed. Reservation by AT, DE, LU, SI and MT.

⁴ FR and NL remarked that the exact IATA terminology should be used for "participating air carriers".

- (d) 'passenger' means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the carrier¹;
- (e) 'reservation systems' means the air carrier's internal reservation system, in which PNR data are collected for the handling of reservations²;
- (f) 'push method' means the method whereby air carriers transfer the required PNR data into the database of the authority requesting them;
- (g) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;
- (h) '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, however, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality³;

¹ GR proposes to add ", which is manifested by the persons' registration in the passengers list". BE queried why crew members were excluded, to which COM replied that their data were not included in PNR data collected by air carriers.

² At the request of EE, COM replied that the reservation system was not the global reservation systems referred to in Regulation EC/80/2009 of 14 January 2009 on a Code of Conduct for computerised reservation systems and repealing Council Regulation (EEC) No 2299/89, but any reservation system.

³ This provision is subject to a general scrutiny reservation. CZ and FR remarked that it was difficult to ascertain the exact legal nature of a possible offence during the intelligence phase

- (i) 'serious transnational crime' means the offences under national law referred to in Article 2(2) of Council Framework Decision 2002/584/JHA¹ 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, and if :
- (i) They are committed in more than one state;
 - (ii) They are committed in one state but a substantial part of their preparation, planning, direction or control takes place in another state;
 - (iii) They are committed in one state but involve an organised criminal group that engages in criminal activities in more than one state; or
 - (iv) They are committed in one state but have substantial effects in another state².

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 authorities³.

¹ DE thought the reference to Framework Decision 2002/584/JHA was too large.

² COM clarified that a "state" did not necessarily need to be a Member State.

³ AT reservation on the proposed decentralised architecture. EE and PL asked whether there would/could be a central component. COM explained that any "hybrid" system with a central component (database or even a mere "exchange platform") would require a Regulation, setting out certain rules applicable thereto. Such "hybrid" system might reduce the costs for air carriers, but would not reduce the costs for Member States as such central component would also need to be staffed. Further to the UK remark that competent public authorities need a basis on which they can network with

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 Directive¹.
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*.

Article 4

Processing of PNR data

1. The PNR data transferred by the air carriers, pursuant to Article 6, in relation to international flights which land on or depart from the territory of each Member State 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 the Annex, 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 or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious transnational 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 process

the PIU, COM stated that, for data protection reasons, it was opposed to the idea of "remote" access by competent authorities of the

¹ DE queried whether a joint PIU would not constitute a circumvention of the rules on international cooperation of Article 7.

PNR data against pre-determined criteria. Member States shall ensure that any positive match resulting from such 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 action^{1 2};

- (b) 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, including international or national databases or national mirrors of Union databases, where they are established on the basis of Union law, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such files. Member States shall ensure that any positive match resulting from such 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 action;
- (c) 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
- (d) 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 transnational crime pursuant to point (a)³.

¹ PL queried whether this did not constitute a common investigative technique as referred to in Article 87(2) c) TFEU, which would consequently imply a need to amend the proposed legal basis for the draft Directive.

² 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.

³ BE, CY, CZ, ES, DE GR, IT, MT, NL, LT, LU, RO, SE and UK challenged the need to distinguish between transnational serious crime and serious crime *tout court* and

3. The assessment of the passengers prior to their scheduled arrival or departure from the Member State 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 a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life¹.
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 points (a) and (b) 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.

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 crime².

pleaded to remove this distinction. COM clarified that the concept of serious crime also encompassed concept transnational serious crime.

¹ BE pleaded in favour of an independent control mechanism regarding the establishment of risk criteria. SI remarked that Article 11 already provided for such mechanism

² UK asked whether an agency, such as the UK Border Agency, whose remit is primarily focused on border control, but also encompasses the investigation of serious crime, could be considered as a competent authority under Article 5. COM replied affirmatively.

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 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 offences, or indications thereof, are detected in the course of enforcement action further to such processing¹.
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 a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life².

¹ ES scrutiny reservation.

² DE asked for a more precise description of the tasks and competences of the PIU.

Article 6

Obligations on air carriers¹

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, 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 international 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 flight². 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.

¹ At the request of ES, COM clarified that it saw no need to describe the role of intermediaries.

² CZ and DE remarked that in case of code-sharing, the operating air carrier often receives PNR data from its code-sharing partner with much delay, sometimes even after the start or the end of the flight and therefore is not able to forward the data in time.

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, 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 crime¹.

Article 7

Exchange of information between Member States²

1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2)(a) and (b), 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 crime³. 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 basis⁴.

¹ FR remarked that ad hoc requests should not be made on a routine basis, but should remain confined to exceptional cases.

² 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.

³ AT proposed to limit this to "the prevention of an immediate and serious threat to public security".

⁴ Addition suggested by SE in order to make such transfers by a receiving PIU in another Member State subject to the same requirement from Article 4(4) for purely domestic transfers.

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 reasoned¹ 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) and (b)².
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 reasoned³ 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 circumstances⁴ in response to a specific threat or a specific investigation or prosecution related to terrorist offences or serious crime.
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 State⁵, shall relate to a

¹ BE and SE request to have the same requirement as in paragraph 4.

² 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.

³ BE and SE request to have the same requirement as in paragraph 4.

⁴ FR requested clarification as to what was covered by this term.

⁵ The need to inform the PIU of such extraordinary requests was emphasised by EE and SE.

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 State¹.

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 time².
6. Exchange of information under this Article may take place using any existing channels for international law enforcement cooperation³ ⁴. 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 the notifications received.

¹ Several Member States (ES, FR, NL) expressed concerns about the need to have a 24/7 availability.

² At the request of FR, COM explained that this related to the possibility to demand, under exceptional circumstances, the earlier transmission of PNR data, provided for in Article 6(4).

³ 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.

⁴ 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 countries¹

A Member State may transfer PNR data stored in accordance with Article 9² 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.

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 30 days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing³.

¹ DE and LV thought the requirement for prior consent of the originating Member State should be clarified.

² The Presidency proposes these additions so as to clarify that that this provision relates solely to the transfers of PNR by the PIU and does not exclude transfers of PNR data by competent authorities in so far as these would be in the possession of PNR data that had already been transferred to them by a PIU in a purely domestic situation.

³ 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.

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 out¹ 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)(d). Access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit² or by judicial authority designated by the Member State³ for the purposes of Article 4(2)(c) 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 prosecution⁴.

For the purposes 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 following⁵:

- 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;

¹ COM acknowledged that term "anonymised" might not be very felicitous, as the procedure of masking out does not prevent that the full data are accessed under the exceptional circumstances set out in this article. The Presidency has therefore replaced it by "masked out".

² AT proposed to add the phrase "subject to supervision by an independent body", but the Presidency deems that the powers of the supervisory authority should be regulated in Article 12.

³ EE proposal.

⁴ 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 Based on AT remark that the list should be exemplative and not exhaustive.

- Frequent flyer information;¹
 - General remarks to the extent that it contains any information which could serve to identify the passenger to whom PNR relate; and
 - 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) and (b) 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 deleted².

¹ AT proposal.

² EE thought this was too narrow, as it excluded storing for statistical purposes. BE queried whether this paragraph implied that in case of a positive match, the data would subsequently need to be 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 Directive¹.

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 applicable².

¹ UK thought penalties should be available both under the law of the Member State which collects the PNR data and the Member State where the air carrier is incorporated. DE also pointed out that in many cases those two states would not be identical and the air carrier might have its seat outside the European Union. NL was of the opinion that the Directive should provide for an EU-wide harmonisation of the sanctions that could be imposed on air carriers, but COM indicated that the proposed legal basis did not allow for it. PL remarked that penalties should not be imposed in case of errors in transmission or failure of transmission due to technical reasons.

² COM clarified that the law enforcement purpose of the transmission of PNR data implied that the Data Protection Directive 95/46 would not 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 revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life shall be prohibited. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately¹.
4. All processing, including receipt of PNR data from air carriers² and all transfer of PNR data by (...) 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 documented³ 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.

¹ Several Member States (CZ, EE, FR, SI and UK) expressed their dissatisfaction with the proposed rules on sensitive data, which, in their view, would defeat the very purpose of a PNR system, as many PNR data could potentially reveal sensitive data. It was suggested that that the use of sensitive data as a selection criterion should be forbidden, rather than the use of such data *tout court*. CZ and UK expressed a preference for the wording in Article 11a of the draft PNR Framework Decision. SI suggested the following drafting: "*In the event that PNR data revealing such information are received by the Passenger Information Unit and this type of information cannot be separated from the PNR data and afterwards deleted, this type of information may exceptionally be processed, but such processing shall not be focused on criteria from the previous sentence*".

² Based on EE suggestion.

³ COM clarified that this included all information covered by such processing: who processed which information, when, etc.

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 international 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 choice¹. The same information shall be made available by the Member States to the public².
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 prohibited³.
7. (...) ⁴.

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.

¹ DE, EE and FR queried how the European Union could impose such obligation on third countries from which air carriers fly to Member States.

² FR expressed a preference for system, like the one regarding SIS, whereby passengers are informed at the airports.

³ 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.

⁴ NL remarked this paragraph should be a separate Article. See Article 15(2).

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 means¹, 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 electronically² 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).

¹ CZ and FR were of the opinion that the Directive should not prescribe the means by which the transmission is to take place.

² FR remarked that some third country air carriers might not have access to electronic transfer lists.

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 powers¹.
2. Where reference is made to this paragraph, Article 4 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.

¹ FR demanded some further explanations as to the exact impact of this reference to comitology.

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 two¹ years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions (...)².

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 Directive³.
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.

¹ AT, CZ, LT and GR scrutiny reservation as to whether two years is a sufficiently long transposition period.

² At the request of several Member States (AT, CY, ES, GR, LV, NL and PT) the reference to the correlation table was deleted.

³ Sentence copied from previous paragraph 7 of Article 12.

Article 16

Transitional provisions

Upon the date referred to in Article 15(1), i.e. two years after the entry into force of this Directive, Member States shall ensure that the PNR data of at least 30% of all flights referred to in Article 6(1) are collected. Until two years after the date referred to in Article 15, Member States shall ensure that the PNR data from at least 60% of all flights referred to in Article 6(1) are collected. Member States shall ensure that from four years after the date referred to in Article 15, the PNR data from all flights referred to in Article 6(1) are collected¹.

Article 17

Review²

On the basis of information provided by the Member States, the Commission shall:

- (a) review the feasibility and necessity of including all internal flights in the scope of this Directive, in the light of the experience gained by those Member States that, in accordance with Article 1a, collect PNR data with regard to internal flights³. The Commission shall submit a report to the European Parliament and the Council within two years after the date mentioned in Article 15(1)⁴;

¹ FR scrutiny reservation on the way in which this provision related to the provisions (in particular Articles 10 and 13).

² PL scrutiny reservation.

³ At the Council meeting of 11 April 2011, the need to have a review clause was emphasised by several delegations. A review clause might potentially also cover other items such as the extension of PNR collection to other modes of transport or the expediency of an EU centralised options for the collection of PNR data.

⁴ EE thought also other modes of transport should be included in the review. NL thought the period of two years should be longer.

- (b) 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, with special attention to the compliance with standard of protection of personal data, the length of the data retention period and the quality of the assessments. It shall also contain the statistical information gathered pursuant to Article 18.

Article 18

Statistical data

1. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units. Such statistics shall as a minimum cover the number of identifications of any persons who may be involved in a terrorist offence or serious crime according to Article 4(2)¹ and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination.
2. These statistics shall not contain any personal data. They shall be transmitted to the Council and the Commission on a yearly basis.

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.

¹ EE thought other Articles (such as Article 9(4)) should also be included.

2. This Directive is without prejudice to any obligations and commitments of Member States¹ 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 UK suggestion, supported by ES and SE.

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