RECITALS COMPROMISES

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 transnational 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 Committee,

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

After having consulted the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

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’34 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’35 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 data36 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.

(4a New) The purpose of this Directive is to ensure security and protect the life and safety of the public, and to create a legal framework for the protection and exchange of PNR data between Member States and law enforcement authorities.

(5) PNR data are necessary to effectively prevent, detect, investigate and prosecute terrorist offences and serious transnational crime and thus enhance internal security.

(6) PNR data can help law enforcement authorities prevent, detect, investigate and prosecute serious transnational crimes, including acts of terrorism, by comparing them with various databases of persons and objects sought, to find the necessary evidence and, where relevant, to find associates of criminals and unravel criminal networks.

(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.

(8) The processing of personal data must be necessary and proportionate to the specific aim 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 transnational crime, it is therefore essential that all Member States introduce provisions laying down obligations on air carriers and non-carrier economic operators operating international flights to or from the territory of the Member States of the European Union.

(11) Air carriers and non-carrier economic carriers who already collect and process PNR data from their passengers for their own commercial purposes. This Directive should not impose any obligation on air carriers and non-carrier economic operators 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 and non-carrier economic operators.

11a New: Non-carrier economic operators, such as travel agencies and tour operators, sell package tours making use of charter flights for which they collect and process PNR data from their customers, yet without necessarily transferring the data to the airline operating the passenger flight.

11b New: Each Member State should be responsible for the costs of running and maintaining its own PNR system, including the costs of appointing and running a competent authority and appointing and running a national supervisory authority. The costs incurred by transferring to national law enforcement agencies and competent

authorities PNR data held by passenger airlines in their reservation systems should be borne by the airlines.

(12) The definition of terrorist offences should be taken from Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism. 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 States. The term serious transnational crime applied in this Directive encompasses the crimes listed in Article 2.

(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 and non-carrier economic operators. Members States should exchange the information through the use of the Secure Information Exchange Network Application (SIENA) system, in order to ensure information sharing and interoperability between Member States.

(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 transnational crime, thereby improving internal security within the Union as well as well as guaranteeing the protecting the fundamental rights of citizens, notably privacy and the protection of personal data by applying high standards in line with the Charter of Fundamental Rights, Convention 108, and the European Convention for Human Rights. Such data sets 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 only contain details on the passenger's reservation and travel itinerary as referred to in this Directive.

(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 and non-carrier economic operators 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 and non-carrier economic operators.

(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 and non-carrier economic operators 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.

(17) The Member States should take all necessary measures to enable air carriers and non-carrier economic operators 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 and non-carrier economic operators failing to meet their obligations regarding the transfer of PNR data and the protection of this 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 transnational crime.

(19) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, in accordance with Articles 8 and 21 of the Charter of Fundamental Rights of the European Union, 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. ¸

(19a new)The result of the processing of PNR data should in no circumstances be used by Member States as a ground to circumvent their obligations international under the 1951 Convention relating to the status of refugees and its 1967 Protocol and should not be used to deny asylum seekers to have safe and effective legal avenues to the EU territory to exercise their right to international protection.

(19b new) Taking fully into consideration the consequences of the judgment of the Court of Justice in Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and others; stresses that the application of this Directive must ensure the full respect of fundamental rights and the right to privacy, the principle of proportionality, and genuinely meet the objectives of what is necessary and proportionate in order to achieve the general interests recognised by the Union and the need to protect the rights and freedoms of others in the fight against terrorism and serious transnational crime. The application of this Directive must be duly justified and the necessary safeguards must be in place in order to ensure the lawfulness of any storage, analysis, transfer and use of PNR data.

(20) Member States should share with other Member States and at European level, as through Europol, the PNR data that they receive where this is necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious transnational crime or the prevention of immediate and serious threats to public security through The Passenger Information Units should in any case transmit the result of the processing of PNR data to the PIUs of other Member States without delay

for further investigation. 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) 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. Such exchange of PNR data between law enforcement and judicial authorities should be governed by the rules on police and judicial cooperation and should not undermine the high level of privacy and protection of personal data in line with the Charter of Fundamental Rights of the European Union, Convention 108 and the European Convention of Human Rights.

20a New. The exchange of information through a secure EU system for the exchange of PNR data between Member States and between Member States and Europol should be guaranteed. The development and operational management of this system could be the responsibility of Europol. A one-stop shop could be created as part of this system to register and transmit the requests for information exchanges. The European Data Protection Supervisor should be responsible for monitoring the processing of the personal data performed through this European system for the exchange of PNR data with Europol.

(21) The period during which PNR data are to be retained should be necessary and proportionate to the purposes of the prevention, detection, investigation and prosecution of terrorist offences and serious transnational 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 and only accessible under very strict and limited conditions.

(21a new) PNR data should be processed to the greatest extent possible in a masked out way in order to ensure the highest level of data protection by making it impossible

for those having access to masked out data to identify a person and to draw conclusions as to what persons are related to that data Re-identifying masked out data is possible only under conditions ensuring a high level of data protection.

(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 matters ('Framework Decision 2008/977/JHA'), and EU data protection law, including the specific data protection requirements set out in this Directive.

(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, EU data protection law, and with the high level of protection offered in the Charter of Fundamental Rights of the European Union, and the European Convention for Human Rights.

(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 that is easily accessible and easy to understand about the collection of PNR data and their transfer to the Passenger Information Unit, as well as their rights as data subjects.

(26) Transfers of PNR data by Member States to third countries should be permitted pursuant to an international agreement or on a case-by-case basis and in full compliance with the provisions laid down by Member States pursuant to 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, as well as the principle of necessity and proportionality of such a transfer, and subject to the high level of protection offered in the Charter of Fundamental Rights of the European Union, Convention 108, and the European Convention for Human Rights. If the national supervisory authority finds the transfer to a third country in breach of any of the principles referred to in this Directive, the national supervisory authority should have the right to suspend the data flow to that third country.

(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 deleted

(29) As a result of the legal and technical differences between national provisions concerning the processing of personal data, including PNR, air carriers and non-carrier economic operators 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 transnational 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 30 days, the collection and use of sensitive data is prohibited. In order to ensure efficiency and a high level of data protection, it must be ensured that an independent national supervisory authority and in particular its Data Protection Officer 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.

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1: This Directive provides for the transfer by air carriers and non-carrier economic operators 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 and with EUROPOL.

2: The PNR data collected in accordance with this Directive may be processed only for the purposes of prevention, detection, investigation and prosecution of terrorist offences and certain types of serious transnational crime in accordance with Article 4(2) or the prevention of immediate and serious threats to public security.

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;

(a New) Non-carrier economic operator means an economic operator, such as travel agencies and tour operators, that provides travel-related services, including the booking of flights for which they collect and process PNR data of passengers;

(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 flights;

(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 carriers 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;

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

(e) ‘reservation systems’ means the air carriers and non-carrier economic operators internal inventory system, in which PNR data are collected for the handling of reservations;

(f) ‘push method’ means the method whereby air carriers and non carrier economic operators transfer the required PNR data listed in the Annex to this Directive 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 on combating terrorism as amended by Council decision 2008/919/JHA.

(h) 'serious transnational crime' means the following offences that are punishable by a custodial sentence or a detention order for a maximum period of at least three years (AM 245, 246) under the national law of a Member State, referred to in Article 2 (2) of Council Framework Decision 2002/584/JHA;

- participation in a criminal organisation,
- trafficking in human beings, facilitation of unauthorised entry and residence, illicit trade in human organs and tissue,
- sexual exploitation of children and child pornography, rape, female genital mutilation
- illicit trafficking in narcotic drugs and psychotropic substances
- illicit trafficking in weapons, munitions and explosives,
- serious fraud, fraud against the financial interests of the EU, laundering of the proceeds of crime, money laundering and counterfeiting currency,
- murder, grievous bodily injured, kidnapping, illegal restraint and hostage-taking, armed robbery,
- serious computer-related crime and cybercrime,
- environmental crime, including illicit

trafficking in endangered animal species and in endangered plant species and varieties,
- forgery of administrative documents and trafficking therein, illicit trafficking in cultural goods, including antiques and works of art,
counterfeiting and piracy of products,
- unlawful seizure of aircraft/ships,
- espionage and treason,
- illicit trade and trafficking in nuclear or radioactive materials and their precursor and in this regard non-proliferation related crimes
- crimes within the jurisdiction of the International Criminal Court

CHAPTER II

RESPONSIBILITES 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 transnational crime and the prevention of immediate and serious threats to public security or a branch of such an authority to act as its 'Passenger Information Unit' responsible for collecting PNR data from the air carriers and non-carrier economic operators, storing them, processing thereof, analysing them and transmitting the result of the analysis to the competent authorities referred to in Article 5. The passenger Information Unit is also responsible for the exchange of PNR data and ~~or~~ the result of the processing thereof with Passenger Information Units of other Member States and EUROPOL in accordance with Article 7, and conducting risk assessment in accordance with Article 4. 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 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 ***jointly*** on the detailed rules for the operation of the Passenger Information Unit and shall respect the requirements laid down in this Directive.

3: Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and ***shall*** at any time update its declaration. The Commission shall publish this information, including any updates, in the Official Journal of the European Union.

DATA PROTECTION OFFICER IN THE PASSENGER INFORMATION UNIT:

1. All Members of the Passenger Information Unite who have access to PNR data shall have received specifically tailored training on processing of PNR data in full compliance with data protection principles and fundamental rights.

2. The passenger information unit shall appoint a data protection officer responsible for the monitoring of the processing of PNR data and the implementation of the related safeguards.

3. Member States shall provide that the data protection officer shall be designated on the basis of professional qualities and in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in this Directive. Member States shall provide that any other professional duties of the data protection officer are compatible with that persons tasks and duties as data protection officer and do not result in a conflict of interest. The Data Protection Officer shall:

(a) Raise awareness and advise staff members of the passenger information unit regarding their obligations for the protection of personal data, including the training of staff and the assignment of responsibilities;
(b) Monitor the implementation and application of data protection provisions contained within this Directive, in particular through conducting random sampling of data processing operations.
(c) Ensure that all documentation is maintained and records kept in accordance with this Directive, and monitor documentation, notification and communication of personal data breaches and report wrong conduct of the data protection requirements set out in this directive to the appropriate authorities;
(d) Monitor the response to requests from the supervisory authority and to cooperate with the supervisory authority, especially on matters relating to data transfers to other Member States or to third countries, and to act as the contact point for the supervisory authority on issues related to the processing of PNR

data; where appropriate the data protection officer should also contact the supervisory authority of his / her own initiative;

(e) Shall be provided by the Member States with the means to perform his / her duties and tasks referred to in this Article effectively and independently.

4. Member States shall provide the data subject with the right to contact the data protection officer, as a single point of contact, on all issues related to the processing of his or her PNR data. Member States shall provide that the name and contact details of the data protection officer are communicated to the supervisory authority and to the public.

Article 4

Processing of PNR data

1. The PNR data transferred by the air carriers and the non-carrier economic operators, 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 and non-carrier economic operators include data beyond those listed in the Annex, the Passenger Information Unit shall delete such data immediately and permanently 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 and where relevant by as well as EUROPOL, as defined in Article 7a new. In carrying out such an assessment, the Passenger Information Unit may process PNR data against pre-determined criteria in accordance with this Directive, and may compare PNR data against relevant databases, including international or national databases or national mirrors of Union databases, where they are established in compliance with Union law, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such files, in line with the requirements set out in paragraph 3. 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;

(b) carrying out an assessment of a passenger 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 a check the Passenger Information Unit may compare PNR data against relevant

databases, including national databases or national mirrors of Union databases, on persons or objects sought or under alert, in accordance with Union, and national rules applicable to such databases for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime. In carrying out such an assessment the passenger Information Unit may compare PNR data against the Schengen Information System and the Visa Information System. 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 based on sufficient evidence, 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 (transnational crimes listed in Article 2.1 (i) or the prevention of an immediate and serious threat to public security, and to provide the competent authorities or where appropriate, EUROPOL 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. 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. This assessment criteria must be targeted, specific, justified, proportionate and fact-based. A regular review shall involve the Data Protection Officer; 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 and regularly reviewed. The assessment criteria shall in no circumstances be based on person’s race or ethnic origin, political opinions, religion or philosophical

beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sex life;

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 by human action.

4a New: The Data Protection Officer shall have access to all data transmitted to the Passenger Information Unit and from the Passenger Information Unit to a competent authority pursuant to Article 5. If the Data Protection Officer considers that transmission of any data was not lawful, he/she shall refer the matter to the Supervisory Authority, who shall have the power to order the receiving competent authority to erase the data.

4b New: The storage, processing and analysis of PNR data shall be carried out and stored exclusively within a secure location within the territory of the Union of the EU or EEA countries.

4c New: Member States shall bear the costs of use, retention and exchange of PNR data.

Article 5

Competent authorities

1. Each Member State shall adopt a list of the competent authorities entitled to request or receive masked out PNR data or the result of the systematic processing of PNR data from the Passenger Information Units in order to examine that information further or take appropriate action for the specific purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime, or the prevention of immediate and serious threats to public security. Europol shall be entitled to receive PNR data or the result of the processing of PNR data from the Passenger Information Units of the Member States within the limits of its mandate and where necessary for the performance of its tasks;

2. Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime or the prevention of immediate and serious threats to public security.

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 shall 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 specific purpose of prevention, detection, investigation or prosecution of terrorist offences and serious transnational crime as defined in point (h) of Article 2 and according to Article 4 (2) for which it was requested or the prevention of immediate and serious threats to public security.

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 processing for which it was originally intended.

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 data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sex life

Article 6

Obligations on air carriers *and non-carrier economic operators* (442 Voss, 443 Gomes)

1. Member States shall adopt the necessary measures to ensure that air carriers and non-carrier economic operators transfer all pushed PNR data as defined in Article 2(c) and specified in the Annex, to the extent that such data are already collected by them in their normal course of business, 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 and the non-carrier economic operator that operates the flight. Where the flight has one or more stop-overs at the airports of the Member States, air carriers and the non-carrier economic operators shall transfer the PNR data to the Passenger Information Units of all the Member States concerned.

2. Air carriers and non-carrier economic operators 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) 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 further passengers to board.

3. Member States shall permit air carriers and non-carrier economic operators 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 and non-carrier economic operators 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, imminent, and actual threat related to terrorist offences or serious transnational crime.

5. Air carriers and non-carriers economic operators shall duly inform passengers of the type of personal data being collected for law enforcement purposes, their rights regarding their data as a passenger. This information shall be provided to passengers proactively, in an easily understandable format.

Article 7

Exchange of information between Member States

1. The Passenger Information Unit of a Member State shall automatically exchange data on the results of the processing of PNR data. Member States shall ensure that the results of the processing of PNR data, either analytical information obtained from PNR data or the results with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2), which is transmitted for further examination to their relevant competent authorities in accordance with Article 4(4), is proactively transmitted without delay by that Passenger Information Unit to the Passenger Information Units of the other Member States. The Passenger Information Unit of the receiving Member States shall transmit such results of the processing of PNR data to their relevant competent authorities, in accordance with Article 4(4). Where appropriate, an alert shall be entered in accordance with Article 36 of the Schengen Information System.

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(1) and, if necessary, also the result of processing thereof, if it has already been prepared pursuant to Article 4(2)(a) and (b). The duly reasoned request for such data shall be strictly limited to the data necessary in this specific case and 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 or the prevention of immediate and serious threats to public security. Passenger Information Units shall provide the requested data as soon as possible using the common protocols and supported data formats. Such a request shall be justified in writing.

4. 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 have been already masked out and 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 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 the most exceptional circumstances in response to a specific real-time threat or a specific investigation or prosecution related to terrorist offences or serious transnational crime or the prevention of immediate and serious threats to public security. Such access to the full PNR data shall be permitted only with the approval of the Head of the requested Passenger Information Unit.

5. Exceptionally, where early access is strictly necessary to respond to a specific and actual threat related to terrorist offences or serious transnational crime or to prevent an immediate and serious threat to public security, the Passenger Information Unit of a Member State shall have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights landing in or departing from the latter's territory at any time, should this data have been retained. This procedure can only cover requests on the PNR data already collected and retained by the Passenger Information Unit which is requested to provide with the data.

6. Exchange of information under this Article shall take place using existing channels for EU and international law enforcement cooperation, in particular Europol and its Secure Information Exchange Network Application (SIENA) and national units under Article 8 of Council Decision 2009/371/JHA of 6 April 2009. 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.

7. When analytical information obtained from PNR is being transferred pursuant to this Directive, the safeguards provided for in paragraph 1 shall be respected.

Article 7a New:

Conditions for access to PNR data by Europol

1. Europol may submit, on a case-by-case basis, an electronic and duly reasoned request to the Passenger Information Unit of any Member State for the transmission of specific PNR data or the results of the processing of specific PNR data, when this is strictly necessary to support and strengthen action by Member States in preventing detecting or investigating a specific terrorist offence or serious transnational crime referred to in Article 2(h) in so far as this offence is covered by Europol's competence pursuant to Council Decision 2009/371/JHA. The reasoned request shall set out reasonable grounds to consider that the transmission of PNR data or the results of the processing of PNR data will substantially contribute to the prevention, detection, investigation or prosecution of the criminal offence in question.

2. Upon receipt of a request by Europol, a court or an independent administrative body of the Member State shall verify, in a timely manner whether all the conditions set out in paragraph 1 are fulfilled, the Passenger Information Unit shall provide the requested data to Europol as soon as practicable.

3. Europol shall inform the Data Protection Officer appointed in accordance with Article 28 of Council Decision 2009/371/JHA of each exchange of information under this Article.

4. Exchange of information under this Article shall take place using the secure information exchange network provided by Europol in accordance with Council Decision 2009/371/JHA. The language used for the request and the exchange of information shall be the one applicable to the secure information exchange network provided by Europol.

Article 8

Transfer of data to third countries

A Member State may transfer PNR data and the results of the processing of PNR data to a third country, only on a case-by-case basis and subject to a duly reasoned request based on sufficient evidence and that the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences, the prevention of immediate and serious threats to public security or the execution of criminal penalties and the receiving competent authority in the third country is responsible for the prevention, investigation, detection or prosecution of criminal offences, the prevention of immediate and serious threats to public security or the execution of criminal penalties; on the condition provided that:

(a) The third country concerned ensures an adequate level of protection as referred to in Directive 95/46/EC for the intended data processing by way of derogation from point (1a) and subject to all the other conditions in this Directive being met;

(b) The Member State from which the data were obtained has given its consent to the transfer in compliance with national law.

In exceptional circumstances w here point 1(a) or (b) do not apply, transfers of PNR data without prior consent in accordance with paragraph 1 shall be permitted only if such transfers are essential for the prevention of an immediate and serious threat to public security of a Member States or a third country or to protect the essential interests of a Member State and prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay, the transfer shall be duly recorded and subject to an ex-post verification.

(a) By way of derogation from the first subparagraph, transfers of data shall be permitted take place on a systematic basis only following the conclusion of an international agreement between a third country and the EU;

(b) The third country or international body concerned ensures an adequate level of protection as referred to in directive 95/46/EC for the intended data processing by way of derogation from point (1a) and subject to all the other conditions of this Directive being met;

(c) In exceptional circumstances where point 1(a) or (b) do not apply, transfers of PNR data without prior consent in accordance with paragraph 1 shall be permitted only if such transfers are essential for the prevention of an immediate and serious threat to public security of a Member States or a third country or to protect the essential interests of a Member State and prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay, the transfer shall be duly recorded and subject to an ex-post verification;

2. Member States shall transfer PNR data to competent authorities of third countries only under terms consistent with this Directive and only upon ascertaining that the use that the recipients intend to make of the PNR is consistent with those terms and safeguards;

3. Save in emergency circumstances, onward transfers to further third countries shall be prohibited in the absence of an international agreement or an adequacy decision. Any such transfer of data from one third country to another in an emergency situation shall take place pursuant to an express understanding incorporating data privacy protections comparable to those applied to PNR data by Member States as provided for in this Directive.

4. PNR data relating to a citizen or a resident of another Member State are being transferred to a third country, the competent authorities of that Member State shall be informed of the matter at the earliest appropriate opportunity.

5. The data protection Officer within the Passenger Information Unit shall be informed each time a Member State transfers PNR data pursuant to this Article. The

Data Protection Officer shall inform, on a regular basis, the Supervisory Authority concerning the transmission of data pursuant to this Article.

Article 9

Period of data retention

1. Member States shall ensure that the PNR data provided by the air carriers and non-carrier economic operators pursuant to Article 4(1), subparagraphs (b) and (c),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 departing.

2. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be retained at the Passenger Information Unit for a further period of five years. During this period, all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such masked out PNR data shall be accessible only to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria according to Article 4(2)(d).

2a New: Re-identification of masked out PNR data and access to the full PNR data shall be authorised by the supervisory authority after consultation of the Data Protection Officer for the purposes of Article 4 (2) (b) and where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk related to terrorist offences or a specific investigation or prosecution related to a crime listed in Article 2.1 or the prevention of an immediate and serious threat to public security. Such access to the full data shall be

allowed for a period of four years after the data has been masked out in cases concerning serious transnational crime and for the entire period of five years in cases concerning terrorist offences.

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:

– Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together;

– Address and contact information;

– 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 permanently 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, subject to human intervention by a member of the Passenger Information Unit, proven to be negative, it shall, however, be stored so as to avoid future ‘false’ positive matches for a maximum period of three years unless the underlying data have not yet

been deleted in accordance with paragraph 3 at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.

Article 10

Penalties against air carriers and non-carrier economic operators

1. 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 and non-carrier economic operators 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 do not process the data in accordance with the data protection rules laid down in this Directive or otherwise infringe the national provisions adopted pursuant to this Directive.

2. ***All data held by air carriers and non-carrier economic operators must ensure that passenger data is held in a secure location, in a secure database on EU territory, on a security accredited computer system, that either meets or exceeds international industrial standards.***

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 protection of their personal data, right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as laid out in national and Union law, and in the implementation of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA. The provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable.

2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of the Council Framework Decision 2008/977/JHA regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.

2a New: Where provisions adopted under national law in implementation of Directive 95/46/EC which provide the passenger with greater rights related to the processing of their data than with this Directive, then these provisions shall apply.

3. Member States shall prohibit the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical

beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sex life shall be prohibited. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately without delay.

4: new Member States shall provide that the Passenger Information Unit maintains documentation of all processing systems and procedures under their responsibility. The documentation shall contain at least:

(a) the name and contact details of the organisation and personnel in the Passenger Information Unit entrusted with the processing of the PNR data, the different levels of access authorisation and the personnel having them;

(b) the requests by competent authorities and Passenger Information Units of other Member States and the recipients of the processed PNR data;

(c) all requests and transfers of data to a third country, the identification of that third country and the legal grounds on which the data are transferred;

(d) the time limits for retention and erasure of different categories of data.

The Passenger Information Unit shall make all documentation available, on request, to the supervisory authority.

4a: New: Member States shall provide that the Passenger Information Unit keeps records of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show in particular the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed PNR data, and the identity and recipients of such data. The records shall be used solely for the purposes of verification, self-monitoring and for ensuring data integrity and data security or for purposes of auditing. The Passenger Information Unit shall make the records available, on request, to the supervisory authority.

Those persons who operate security controls, who access and analyse the PNR data, and who operate the data logs, must be security cleared and security trained. Each such person shall have a profile which defines and limits what he or she is authorised to see according to the nature of his or her work, role, and legal entitlement.
The records shall be kept for a period of four years, unless the underlying data have not yet been deleted in accordance with Article 9(3) at the expiry of those four years, in which case the logs shall be kept until the underlying data are deleted.

4b New: Member States shall provide that the Passenger Information Unit implements appropriate technical and organisational measures and procedures to ensure a high level of security appropriate to the risks represented by the processing and the nature of the PNR data to be protected.

4c New: Member States shall provide that when a personal data breach is likely to adversely affect the protection of the personal data and / or the privacy of the data subject, the Passenger Information Unit, shall communicate the personal data breach to the data subject and to the national data protection supervisor without undue delay.

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 transnational crime, the possibility of exchanging and sharing such data and their data protection rights, such as the right to access, correction, erasure and blocking of data, and in particular the right to complain to a national data protection supervisory authority of their choice.

5a New: Member States shall also ensure that the Passenger Information Unit provides the data subject with the information laid out in Article 11 paragraph 5, as well as provide information on how to exercise these rights.

6 New. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of all the provisions of this Directive and 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. National supervisory authorities shall take disciplinary action against persons responsible for any such intentional privacy breach, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.

7 New: Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited. Any wrong conduct should be sanctioned.

Article 12

National supervisory authority

1. Each Member State shall provide that the national supervisory authority established in implementation of Article 25 of Framework Decision 2008/977/JHA shall 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.

DUTIES & POWERS OF THE NATIONAL SUPERVISORY AUTHORITY

1 New: The national supervisory authority of each Member State shall be responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights in relation to the processing of their personal data. The national supervisory authorities shall:

(a) hear complaints lodged by any data subject, investigates, the matter and informs the data subjects of the progress and the outcome of the complaints within a reasonable time period, in particular where further investigation or coordination with another supervisory authority is necessary; those complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

(b) shall exercise effective powers of oversight, investigation, intervention and review, and have the power to refer infringements of law related to this Directive for prosecution or disciplinary action, when appropriate.

(c) check the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint, and informs the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable time period; Member States shall provide a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat;

(d) Monitor relevant developments, insofar as they have an impact on the protection of person data, in particular the development of information and communication technologies.

2. The supervisory authority shall, upon request advise any data subject in exercising the rights laid down in provisions adopted pursuant to this Directive and, where appropriate, co-operate with supervisory authorities in other Member States to this end.

3. For complaints referred to in point (2b) the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

4. Member States shall provide that the performance of the duties of the supervisory authority shall be free for the data subject, or where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a reasonable fee.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premise and infrastructure necessary for the effective performance of its duties and powers.

6. Each Member States shall ensure that the supervisory authority must have its own staff which shall be appointed by and subject to the direction of the head of the supervisory authority.

7. Members of the supervisory authority in the performance of their duties, shall neither seek nor take instruction from anybody, and maintain complete independence and impartiality;

CHAPTER IV

IMPLEMENTING MEASURES

Article 13

Common protocols and supported data formats

1. All transfers of PNR data by air carriers, and non-carrier economic operators to the Passenger Information Units for the purposes of this Directive shall be made by electronic means that provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. In the event of technical failure, the PNR data shall be transferred by any other appropriate means whilst maintaining the same level of security and in full compliance with EU data protection law.

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 and non-carrier economic operators to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.

3. The list of accepted common protocols and supported data formats shall be drawn up and, if need be, adjusted, by delegated act as stated in Article 14.

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

Delegated Acts

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 14 shall be conferred on the Commission for a period of [X] years from the entry into force of this Directive. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the [X] year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 14 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 14 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

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 two years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive. 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 16

Transitional provisions

DELETED ARTICLE.

Article 17

Review

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

(a) 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,

(b) there shall be special attention to the compliance with standard of protection of personal data, the necessity and proportionality of the collection and processing of PNR data for each of the stated purposes, the length of the data retention period and the quality of the assessments and the effectiveness of the sharing of data between the Member States, and the quality of the assessment including with regard to the statistical information gathered pursuant to Article 18. It shall also contain the statistical information gathered pursuant to Article 18.

(c) New: The Commission shall submit an initial evaluation report after consultation with the relevant EU agencies to the European Parliament and the Council within two years after the date of transposition of this Directive;

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 transnational serious crime according to Article 4(2) and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination; including the number of investigation and convictions that have resulted from the collection of PNR data in each Member State.

2. These statistics shall not contain any personal data. They shall be transmitted to the Commission, the Council and the European Parliament every two years.

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.

1New: This Directive applies without prejudice to the Council Framework decision 2008 / 977JHA.

2. This Directive is without prejudice to any obligations and commitments 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

ANNEX

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) A number of amendments relating to the general remarks box.

(13) Ticketing field information, including ticket number, date of ticket issuance and oneway 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