Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[(1)],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure[(2)],

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 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'[(3)] calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

(3) In its Communication of 21 September 2010'On the global approach to transfers of passenger name record (PNR) data to third countries', the Commission outlined a number of core elements of a Union policy in this area.

(4) Council Directive 2004/82/EC[(4)] regulates the transfer of advance passenger information (API) data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration.

(5) The objectives of this Directive are, inter alia, to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.

(6) Effective use of PNR data, for example by comparing PNR data against various databases on persons and objects sought, is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks.

(7) Assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is necessary, the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system.

(8) Air carriers already collect and process their passengers' PNR data 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 any obligation on passengers to provide any data in addition to that already being provided to air carriers.

(9) Some air carriers retain as part of the PNR data the API data they collect, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that where air carriers collect API data, they transfer it irrespective of whether they retain API data by different technical means as for other PNR data.

(10) To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is essential that all Member States introduce provisions laying down obligations on air carriers operating extra-EU flights to transfer PNR data they collect, including API data. Member States should also have the possibility to extend this obligation to air carriers operating intra-EU flights. Those provisions should be without prejudice to Directive 2004/82/EC.

(11) The processing of personal data should be proportionate to the specific security goals pursued by this Directive.

(12) The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA[(5)]. The definition of serious crime should encompass the categories of offence listed in Annex II to this Directive.

(13) PNR data should be transferred to a single designated passenger information unit (‘PIU’) in the relevant Member State, so as to ensure clarity and reduce costs for air carriers. The PIU may have different branches in one Member State and Member States may also establish one PIU jointly. Member States should exchange

the information among each other through relevant information exchange networks to facilitate information sharing and ensure interoperability.

(14) Member States should bear the costs of using, retaining and exchanging PNR data.

(15) A list of the PNR data to be obtained by a PIU 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, in particular privacy and the protection of personal data. To that end, high standards should be applied in accordance with the Charter of Fundamental Rights of the European Union (the 'Charter'), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention No 108'), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR'). Such a list should not be based on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation. The PNR data should only contain details of passengers' reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security.

(16) There are two possible methods of data transfer currently available: the 'pull' method, under which the competent authorities of the Member State requiring the PNR data can access the air carrier's reservation system and extract ('pull') a copy of the required PNR 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 level of data protection and should be mandatory for all air carriers.

(17) The Commission supports the International Civil Aviation Organisation (ICAO) guidelines on PNR. Those guidelines should therefore be the basis for adopting the supported data formats for transfers of PNR data by air carriers to Member States. In order to ensure uniform conditions for the implementation of supported data formats and of relevant protocols applicable to the transfer of data from air carriers, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[(6)].

(18) Member States should take all necessary measures to enable air carriers to fulfil their obligations under this Directive. Effective, proportionate and dissuasive 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.

(19) Each Member State should be responsible for assessing the potential threats related to terrorist offences and serious crime.

(20) 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 significantly affects that person should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Articles 8 and 21 of the Charter, no

such decision should discriminate on any grounds such as a person's sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The Commission should also take those principles into account when reviewing the application of this Directive.

(21) The result of processing PNR data should in no circumstances be used by Member States as a ground to circumvent their international obligations under the Convention of 28 July 1951 relating to the Status of Refugees as amended by the Protocol of 31 January 1967, nor should it be used to deny asylum seekers safe and effective legal avenues into the territory of the Union to exercise their right to international protection.

(22) Taking fully into consideration the principles outlined in recent relevant case law of the Court of Justice of the European Union, the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality. It should also genuinely meet the objectives of necessity and proportionality 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 terrorist offences and serious crime. The application of this Directive should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data.

(23) Member States should exchange the PNR data that they receive among each other and with Europol, where this is deemed necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime. PIUs should, where appropriate, transmit the result of processing PNR data without delay to the PIUs of other Member States for further investigation. The provisions of this Directive should be without prejudice to other Union instruments on the exchange of information between police and other law enforcement authorities and judicial authorities, including Council Decision 2009/371/JHA[(7)] and Council Framework Decision 2006/960/JHA[(8)]. Such exchange of PNR data should be governed by the rules on police and judicial cooperation and should not undermine the high level of protection of privacy and of personal data required by the Charter, Convention No 108 and the ECHR.

(24) A secure exchange of information regarding PNR data between the Member States should be ensured through any of the existing channels for cooperation between the competent authorities of the Member States, and in particular with Europol through Europol's Secure Information Exchange Network Application (SIENA).

(25) The period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations. To avoid disproportionate use, after the initial retention period the PNR data should be depersonalised through masking out of data elements. To ensure the highest level of data protection, access to the full PNR data, which enable direct identification of the data subject, should be granted only under very strict and limited conditions after that initial period.

(26) 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 national law, irrespective of the data retention periods set out in this Directive.

(27) The processing of PNR data in each Member State by the PIU and by competent authorities should be subject to a standard of protection of personal data under national law in line with Council Framework Decision 2008/977/JHA[(9)] and the specific data protection requirements laid down in this Directive. References to Framework Decision 2008/977/JHA should be understood as references to legislation currently in force as well as to legislation that will replace it.

(28) Taking into consideration the right to the protection of personal data, the rights of data subjects concerning the processing of their PNR data, such as the rights of access, rectification, erasure and restriction and the rights to compensation and judicial redress, should be in line both with Framework Decision 2008/977/JHA and with the high level of protection provided by the Charter and the ECHR.

(29) Taking into account the right of passengers to be informed of the processing of their personal data, Member States should ensure that passengers are provided with accurate information that is easily accessible and easy to understand about the collection of PNR data, their transfer to the PIU and their rights as data subjects.

(30) This Directive is without prejudice to Union and national law on the principle of public access to official documents.

(31) Transfers of PNR data by Member States to third countries should be permitted only 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. They should also be subject to the principles of necessity and proportionality and to the high level of protection provided by the Charter and by the ECHR.

(32) 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 of the provisions adopted by the Member States pursuant to this Directive.

(33) This Directive does not affect the possibility for Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services — including the booking of flights — for which they collect and process PNR data, or from transportation providers other than those specified in this Directive, provided that such national law complies with Union law.

(34) This Directive is without prejudice to current Union rules on the way border controls are carried out or to Union rules regulating entry and exit from Union territory.

(35) As a result of the legal and technical differences between national provisions concerning the processing of personal data, including PNR data, air carriers are and will be faced with different requirements regarding the types of information to be transmitted and the conditions under which it needs to be provided to competent national authorities. Those 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. It is therefore necessary to establish at Union level a common legal framework for the transfer and processing of PNR data.

(36) This Directive respects the fundamental rights and the principles of the Charter, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof; it should therefore be implemented accordingly. This Directive is compatible with data protection principles and its provisions are in line with Framework Decision 2008/977/JHA. Furthermore, to comply with the proportionality principle, on specific issues this Directive provides for stricter rules on data protection than Framework Decision 2008/977/JHA.

(37) The scope of this Directive is as limited as possible since: it provides for the retention of PNR data in the PIUs for a period of time not exceeding five years, after which the data should be deleted; it provides for the data to be depersonalised through masking out of data elements after an initial period of six months; and it prohibits the collection and use of sensitive data. To ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority and, in particular, a data protection officer are responsible for advising and monitoring the way PNR data are processed. All processing of PNR data should be logged or documented for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. Member States should also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.

(38) Since the objectives of this Directive — namely the transfer of PNR data by air carriers and processing of those data for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime — cannot be sufficiently achieved by the Member States, but can rather 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 those objectives.

(39) 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 take part in the adoption and application of this Directive.

(40) 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.

(41) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[10] and delivered an opinion on 25 March 2011,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

General provisions

Article 1

Subject-matter and scope

1 This Directive provides for:

a the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights,

b the processing of the data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States.

2 PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2).

Article 2

Application of this Directive to intra-EU flights

1 If a Member State decides to apply this Directive to intra-EU flights, it shall notify the Commission in writing. A Member State may give or revoke such a notification at any time. The Commission shall publish that notification and any revocation of it in the *Official Journal of the European Union*.

2 Where a notification referred to in paragraph 1 is given, all the provisions of this Directive shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights.

3 A Member State may decide to apply this Directive only to selected intra-EU flights. In making such a decision, the Member State shall select the flights it considers necessary in order to pursue the objectives of this Directive. The Member State may decide to change the selection of intra-EU flights at any time.

Article 3

Definitions

For the purposes of this Directive the following definitions apply:

(1) ‘air carrier’ means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air;

(2) 'extra-EU flight' means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries;

(3) 'intra-EU flight' means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country;

(4) 'passenger' means any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person's registration in the passengers list;

(5) 'passenger name record' or 'PNR' 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 used to check passengers onto flights, or equivalent systems providing the same functionalities;

(6) 'reservation system' means the air carrier's internal system, in which PNR data are collected for the handling of reservations;

(7) 'push method' means the method whereby air carriers transfer PNR data listed in Annex I into the database of the authority requesting them;

(8) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(9) 'serious crime' means the offences listed in Annex II that 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;

(10) 'to depersonalise through masking out of data elements' means to render those data elements which could serve to identify directly the data subject invisible to a user.

CHAPTER II

Responsibilities of the Member States

Article 4

Passenger information unit

1 Each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its passenger information unit ('PIU').

2 The PIU shall be responsible for:

a collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities referred to in Article 7;

b exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol in accordance with Articles 9 and 10.

3 Staff members of a PIU may be seconded from competent authorities. Member States shall provide the PIUs with adequate resources for them to fulfil their tasks.

4 Two or more Member States (the participating Member States) may establish or designate a single authority to serve as their PIU. Such PIU shall be established in one of the participating Member States and shall be considered the national PIU of all participating Member States. The participating Member States shall agree jointly on the detailed rules for the operation of the PIU and shall respect the requirements laid down in this Directive.

5 Within one month of the establishment of its PIU, each Member State shall notify the Commission thereof, and may modify its notification at any time. The Commission shall publish the notification and any modifications of it in the *Official Journal of the European Union*.

Article 5

Data protection officer in the PIU

1 The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.

2 Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently.

3 Member States shall ensure that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.

Article 6

Processing of PNR data

1 The PNR data transferred by the air carriers shall be collected by the PIU of the relevant Member State as provided for in Article 8. Where the PNR data transferred by air carriers include data other than those listed in Annex I, the PIU shall delete such data immediately and permanently upon receipt.

2 The PIU shall process PNR data only for the following purposes:

a carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;

b responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and

c analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime.

3 When carrying out the assessment referred to in point (a) of paragraph 2, the PIU may:

a compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases; or

b process PNR data against pre-determined criteria.

4 Any assessment of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 against pre-determined criteria shall be carried out in a non-discriminatory manner. Those pre-determined criteria must be targeted, proportionate and specific. Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. The criteria shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

5 Member States shall ensure that any positive match resulting from the automated processing of PNR data conducted under point (a) of paragraph 2 is individually reviewed by non-automated means to verify whether the competent authority referred to in Article 7 needs to take action under national law.

6 The PIU of a Member State shall transmit the PNR data of persons identified in accordance with point (a) of paragraph 2 or the result of processing those data for further examination to the competent authorities referred to in Article 7 of the same Member State. Such transfers shall only be made on a case-by-case basis and, in the event of automated processing of PNR data, after individual review by non-automated means.

7 Member States shall ensure that the data protection officer has access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority.

8 The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States.

9 The consequences of the assessments of passengers referred to in point (a) of paragraph 2 of this Article shall not jeopardise the right of entry of persons enjoying the Union right of free movement into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council[(11)]. In addition, where assessments are carried out in relation to intra-EU flights between Member States to which Regulation (EC) No 562/2006 of the European Parliament and of the Council[(12)] applies, the consequences of such assessments shall comply with that Regulation.

Article 7

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 processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

2 The authorities referred to in paragraph 1 shall be authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime.

3 For the purpose of Article 9(3), each Member State shall notify the Commission of the list of its competent authorities by 25 May 2017, and may modify its notification at any time. The Commission shall publish the notification and any modifications of it in the *Official Journal of the European Union*.

4 The PNR data and the result of processing those data received by the PIU may be further processed by the competent authorities of the Member States only for the specific purposes 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 processing.

6 The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

Article 8

Obligations on air carriers regarding transfers of data

1 Member States shall adopt the necessary measures to ensure that air carriers transfer, by the ‘push method’, the PNR data listed in Annex I, to the extent that they have already collected such data in the normal course of their business, to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where an extra-EU flight has one or more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned. This also applies where an intra-EU flight has one or more stopovers at the airports of different Member States, but only in relation to Member States which are collecting PNR data from intra-EU flights.

2 In the event that the air carriers have collected any advance passenger information (API) data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the ‘push method’, those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data.

3 Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the examination procedure referred to in Article 17(2) 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 flight departure time; 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 passengers to board or leave.

4 Member States shall permit air carriers to limit the transfer referred to in point (b) of paragraph 3 to updates of the transfers referred to in point (a) of that paragraph.

5 Where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, air carriers shall, on a case by case basis, transfer PNR data at other points in time than those mentioned in paragraph 3, upon request from a PIU in accordance with national law.

Article 9

Exchange of information between Member States

1 Member States shall ensure that, with regard to persons identified by a PIU in accordance with Article 6(2), all relevant and necessary PNR data or the result of processing those data is transmitted by that PIU to the corresponding PIUs of the other Member States. The PIUs of the receiving Member States shall transmit, in accordance with Article 6(6), the received information to their competent authorities.

2 The PIU of a Member State shall have the right to request, if necessary, that the PIU of any other Member State provide it with PNR data that are kept in the latter's database and that have not yet been depersonalised through masking out of data elements under Article 12(2), and also, if necessary, the result of any processing of those data, if it has already been carried out pursuant to point (a) of Article 6(2). Such a request shall be duly reasoned. It may be based on any one data element or a combination of such elements, as deemed necessary by the requesting PIU for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime. PIUs shall provide the requested information as soon as practicable. In the event that the requested data have been depersonalised through masking out of data elements in accordance with Article 12(2), the PIU shall only provide the full PNR data where it is reasonably believed that it is necessary for the purpose referred to in point (b) of Article 6(2) and only when authorised to do so by an authority referred to in point (b) of Article 12(3).

3 The competent authorities of a Member State may request directly the PIU of any other Member State to provide them with PNR data that are kept in the latter's database only when necessary in cases of emergency and under the conditions laid down in paragraph 2. The requests from the competent authorities shall be reasoned. A copy of the request shall always be sent to the PIU of the requesting Member State. In all other cases, the competent authorities shall channel their requests through the PIU of their own Member State.

4 Exceptionally, where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the PIU of a Member State shall have the right to request that the PIU of another Member State obtain PNR data in accordance with Article 8(5) and provide it to the requesting PIU.

5 Exchange of information under this Article may take place using any existing channels for cooperation between the competent authorities of Member States. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when giving their notifications in accordance with Article 4(5), also inform the Commission of the details of the contact points to which requests may be sent in cases of emergency. The Commission shall communicate such details to the Member States.

Article 10

Conditions for access to PNR data by Europol

1 Europol shall be entitled to request PNR data or the result of processing those data from the PIUs of Member States within the limits of its competences and for the performance of its tasks.

2 Europol may submit, on a case-by-case basis, an electronic and duly reasoned request to the PIU of any Member State through the Europol National Unit for the transmission of specific PNR data or the result of processing those data. Europol may submit such a request when this is strictly necessary to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious crime in so far as such an offence or crime is within Europol's competence pursuant to Decision 2009/371/JHA. That request shall set out reasonable grounds on the basis of which Europol considers that the transmission of PNR data or the result of processing PNR data will substantially contribute to the prevention, detection or investigation of the criminal offence concerned.

3 Europol shall inform the data protection officer appointed in accordance with Article 28 of Decision 2009/371/JHA of each exchange of information under this Article.

4 Exchange of information under this Article shall take place through SIENA and in accordance with Decision 2009/371/JHA. The language used for the request and the exchange of information shall be that applicable to SIENA.

Article 11

Transfer of data to third countries

1 A Member State may transfer PNR data and the result of processing such data that are stored by the PIU in accordance with Article 12 to a third country, only on a case-by-case basis and if:

a the conditions laid down in Article 13 of Framework Decision 2008/977/JHA are met;

b the transfer is necessary for the purposes of this Directive referred to in Article 1(2);

c the third country agrees to transfer the data to another third country only where it is strictly necessary for the purposes of this Directive referred to in Article 1(2) and only with the express authorisation of that Member State; and

d the same conditions as those laid down in Article 9(2) are met.

2 Notwithstanding Article 13(2) of Framework Decision 2008/977/JHA, transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances and only if:

a such transfers are essential to respond to a specific and actual threat related to terrorist offences or serious crime in a Member State or a third country, and

b prior consent cannot be obtained in good time.

The authority responsible for giving consent shall be informed without delay and the transfer shall be duly recorded and subject to an *ex-post* verification.

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

4 The data protection officer of the PIU of the Member State that has transferred the PNR data shall be informed each time the Member State transfers PNR data pursuant to this Article.

Article 12

Period of data retention and depersonalisation

1 Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.

2 Upon expiry of a period of six months after the transfer of the PNR data referred to in paragraph 1, all PNR data shall be depersonalised through masking out the following data elements which could serve to identify directly the passenger to whom the PNR data relate:

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

b address and contact information;

c all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;

d frequent flyer information;

e general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

f any API data that have been collected.

3 Upon expiry of the period of six months referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is:

a reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2) and

b approved by:

(i) a judicial authority; or

(ii) another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an *ex-post* review by that data protection officer.

4 Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case the retention of such data by the competent authority shall be regulated by national law.

5 The result of the processing referred to in point (a) of Article 6(2) shall be kept by the PIU only as long as necessary to inform the competent authorities and, in accordance with Article 9(1), to inform the PIUs of other Member States of a positive match. Where the result of automated processing has, further to individual review by non-automated means as referred to in Article 6(5), proven to be negative, it may, however, be stored so as to avoid future ‘false’ positive matches for as long as the underlying data are not deleted under paragraph 4 of this Article.

Article 13

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, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in Union and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision 2008/977/JHA. Those Articles shall therefore apply.

2 Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of 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 This Directive is without prejudice to the applicability of Directive 95/46/EC of the European Parliament and of the Council[(13)] to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data.

4 Member States shall prohibit the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.

5 Member States shall ensure that the PIUs maintain documentation relating to all processing systems and procedures under their responsibility. That documentation shall contain at least:

a the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation;

b the requests made by competent authorities and PIUs of other Member States;

c all requests for and transfers of PNR data to a third country.

The PIU shall make all documentation available, upon request, to the national supervisory authority.

6 Member States shall ensure that the PIU keeps records of at least the following processing operations: collection, consultation, disclosure and 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 identity of the person who consulted or disclosed the PNR data and the identity of recipients of those data. The records shall be used solely for the purposes of verification, of self-monitoring, of ensuring data integrity and data security or of auditing. The PIU shall make the records available, upon request, to the national supervisory authority.

Those records shall be kept for a period of five years.

7 Member States shall ensure that their PIU 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.

8 Member States shall ensure that where a personal data breach is likely to result in a high risk for the protection of the personal data or affect the privacy of the data subject adversely, the PIU shall communicate that breach to the data subject and to the national supervisory authority without undue delay.

Article 14

Penalties

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented.

In particular, Member States shall lay down rules on penalties, including financial penalties, against air carriers which do not transmit data as provided for in Article 8 or do not do so in the required format.

The penalties provided for shall be effective, proportionate and dissuasive.

Article 15

National supervisory authority

1 Each Member State shall provide that the national supervisory authority referred to in Article 25 of Framework Decision 2008/977/JHA is responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. Article 25 of Framework Decision 2008/977/JHA shall apply.

2 Those national supervisory authorities shall conduct activities under paragraph 1 with a view to protecting fundamental rights in relation to the processing of personal data.

3 Each national supervisory authority shall:

a deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period;

b verify 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 referred to in point (a).

4 Each national supervisory authority shall, upon request, advise any data subject on the exercise of the rights laid down in provisions adopted pursuant to this Directive.

CHAPTER III

Implementing measures

Article 16

Common protocols and supported data formats

1 All transfers of PNR data by air carriers to the PIUs for the purposes of this Directive shall be made by electronic means that provide sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. In the event of a technical failure, the PNR data may be transferred by any other appropriate means provided that the same level of security is maintained and Union data protection law is fully complied with.

2 As of one year after the date the Commission first adopts common protocols and supported data formats in accordance with paragraph 3, all transfers of PNR data by air carriers to the PIUs for the purposes of this Directive shall be made electronically using secure methods conforming to those common protocols. Such protocols shall be common to all transfers to ensure the security of the PNR data during transfer. The PNR data shall be transferred 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 PIU the common protocol and data format that they intend to use for their transfers.

3 The list of common protocols and supported data formats shall be drawn up and, if necessary, adjusted by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 17(2).

4 Paragraph 1 shall apply for as long as the common protocols and supported data formats referred to in paragraphs 2 and 3 are not available.

5 Within one year from the date of the adoption of the common protocols and supported data formats referred to in paragraph 2, each Member State shall ensure that the necessary technical measures are adopted to be able to use those common protocols and data formats.

Article 17

Committee procedure

1 The Commission shall be assisted by a committee. That Committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2 Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

CHAPTER IV

Final provisions

Article 18

Transposition

1 Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 25 May 2018. They shall immediately inform the Commission thereof.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2 Member States shall communicate to the Commission the text of the main measures of national law which they adopt in the field covered by this Directive.

Article 19

Review

1 On the basis of information provided by the Member States, including the statistical information referred to in Article 20(2), the Commission shall by 25 May 2020 conduct a review of all the elements of this Directive and submit and present a report to the European Parliament and to the Council.

2 In conducting its review, the Commission shall pay special attention to:

a compliance with the applicable standards of protection of personal data,

b the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive,

c the length of the data retention period,

d the effectiveness of exchange of information between the Member States, and

e the quality of the assessments including with regard to the statistical information gathered pursuant to Article 20.

3 The report referred to in paragraph 1 shall also include a review of the necessity, proportionality, and effectiveness of including within the scope of this Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights. The Commission shall take into account the experience gained by Member States, especially those Member States that apply this Directive to intra-EU flights in accordance with Article 2. The report shall also consider the necessity of including non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services, including the booking of flights, within the scope of this Directive.

4 If appropriate, in light of the review conducted pursuant to this Article, the Commission shall make a legislative proposal to the European Parliament and to the Council with a view to amending this Directive.

Article 20

Statistical data

1 On a yearly basis, Member States shall provide the Commission with a set of statistical information on PNR data provided to the PIUs. These statistics shall not contain any personal data.

2 The statistics shall as a minimum cover:

a the total number of passengers whose PNR data have been collected and exchanged;

b the number of passengers identified for further examination.

Article 21

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

that are in force on 24 May 2016, in so far as such agreements or arrangements are compatible with this Directive.

2 This Directive is without prejudice to the applicability of Directive 95/46/EC to the processing of personal data by air carriers.

3 This Directive is without prejudice to any obligations and commitments of Member States or of the Union by virtue of bilateral or multilateral agreements with third countries.

Article 22

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, 27 April 2016.

For the European Parliament

The President

M. SCHULZ

For the Council

The President

J.A. HENNIS-PLASSCHAERT

ANNEX I

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 the PNR
18. Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)
19. All historical changes to the PNR listed in numbers 1 to 18.

ANNEX II

List of offences referred to in point (9) of Article 3

1. participation in a criminal organisation,
2. trafficking in human beings,

3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,
14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,
22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.

(**1**) OJ C 218, 23.7.2011, p. 107.

(**2**) Position of the European Parliament of 14 April 2016 (not yet published in the Official Journal) and decision of the Council of 21 April 2016.

(**3**) OJ C 115, 4.5.2010, p. 1.

(**4**) Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

(**5**) Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (OJ L 164, 22.6.2002, p. 3).

(**6**) 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 (OJ L 55, 28.2.2011, p. 13).

(**7**) Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

(**8**) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).

(**9**) Council 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 (OJ L 350, 30.12.2008, p. 60).

(**10**) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(**11**) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(**12**) Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 105, 13.4.2006, p. 1).

(**13**) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).