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

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[(1)]. 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[(2)] 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[(3)] 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.

(**1**) 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).

(**2**) 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).

(**3**) 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).