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:

(**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).