Council of the European Union

Brussels, 2 December 2015
(OR. en)

14670/15

Interinstitutional File: 2011/0023 (COD)

LIMITE

GENVAL 63
AVIATION 145
DATAPROTECT 218
ENFOPOL 372
CODEC 1608

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	14024/15
Subject:	Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - approval of final compromise text

1. On 4 February 2011, the Commission submitted to the European Parliament and the Council the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences, set out in 6007/11.

2. On 26 April 2012, the Council agreed on a general approach, set out in 9916/15.

3. On 15 July 2015, the LIBE Committee adopted the second KIRKHOPE report on the EU PNR Directive (presented on 26 February 2015), as well as the mandate to open negotiations with the Council.[1]

[1] The EP negotiating team is composed as follows: Mr MORAES (S&D), LIBE Chair, Mr KIRKHOPE (ECR), rapporteur, and the shadow rapporteurs Mr VOSS (EPP), Ms SIPPEL (S&D), Ms IN'T VELD (ALDE), Ms ERNST (GUE/NGL), Mr ALBRECHT (Greens/EFA), Ms WINBERG (EFDD).

4. On 19 November 2015, COREPER was given a state of play on the negotiations of the Commission's proposal on an EU PNR-system. The background information on the negotiations was set out in14024/15.

5. In the Council Conclusions[2] adopted at the extraordinary JHA Council of 20 November 2015, the Council in point 2 reiterated "*the urgency and priority to finalise an ambitious EU PNR before the end of 2015, which should include internal flights in its scope, provide for a sufficiently long data period during which PNR data can be retained in non-masked-out form and should not be limited to crimes of a transnational nature*."

6. The negotiations with the EP, which started in September 2015, take place in a highly unusual institutional setting in the sense that the Kirkhope report voted on 15 July 2015 by the LIBE Committee was not supported by a majority of the shadow rapporteurs (only the EPP shadow rapporteur supported it)[3], but by a 'heterogeneous' majority of LIBE MEPs across-party lines.

7. The Presidency has had five informal trilogues with the EP on the following dates: 24 and 29 September, 9 and 17 November, and 2 December 2015. Technical meetings have taken place on 16 October, 13, 19 and 27 November.

8. At the informal trilogue of 2 December 2015, a compromise package has been reached with the rapporteur, the text of which is set out in the Annex to this note. Text underlined reflects changes to the Commission proposal stemming from the Council general approach, and text in bold without underlining reflects Parliament amendments already discussed by either the Working Party (GENVAL) or JHA Counsellors. Changes to the text after trilogue of 2 December 2015 are indicated in ***underlined bold italics***.

---

[2] 14406/15.

[3] The EP negotiating team is composed as follows: Mr MORAES (S&D), LIBE Chair, Mr KIRKHOPE (ECR), rapporteur, and the shadow rapporteurs Mr VOSS (EPP), Ms SIPPEL (S&D), Ms IN'T VELD (ALDE), Ms ERNST (GUE/NGL), Mr ALBRECHT (Greens/EFA), Ms WINBERG (EFDD).

9. On the main political issues, the compromise text consists of the following elements:

a) Concerning the scope, a single list of offences has been agreed with the Parliament and the element of "transnational" has been left out from the definition of serious crime, while acknowledging in recital (12) that such crimes will often have a cross-border element.

b) On data protection, in order to incorporate part of the EP amendments, the text is now more detailed than the April 2012 general approach of the Council and includes, *inter alia*, an article (3a) on a data protection officer (DPO) in the Passenger Information Unit (PIU). By way of a dynamic reference to the 2008 Data Protection Framework Decision, it will be ensured that the future data protections instruments that will replace the current ones will also become applicable (Article 11 and recital 23).

c) Recital 28 of the Directive, as it currently stands, permits, but does not oblige Member State to include non-carrier economic operators under their domestic law, in a system of collection and processing of PNR data from non-carrier economic operators. Article 17 calls upon the Commission to include this matter in its review of the future PNR system.

d) The text agreed contains the voluntary inclusion of intra-EU flights under the terms set out in the general approach of the Council.

e) The EP is demanding that the initial storage period during which the PNR data are fully accessible/not masked out is reduced to six months. Referring to the 2011 EU-US Agreement, to which the Council has agreed and the EP has given its consent and in which the initial retention period is also six months, the rapporteur has indicated that he has no flexibility to agree on a longer retention period. However, Article 9(3) allows to 'repersonalise' masked-out data under conditions compatible with operational requirements.

10. The Presidency considers that the compromise text out in the Annex represents a well-balanced compromise that takes into account the major concerns and priorities of all parties involved. It therefore invites COREPER to approve the compromise agreement and take the procedural decision, according to Article 19(7)(k) of the Council's rules of procedure, to inform the Parliament accordingly through a letter.

11. For these reasons, COREPER is invited to:

a) approve the final compromise text of the Directive, as set out in the Annex to this note;

b) mandate the Presidency to inform the European Parliament that, should the European Parliament adopt its position at first reading in the exact form as set out in the final compromise text, the Council would approve the European Parliament's position and the Directive shall be adopted in the wording which corresponds to the European Parliament's position, subject to legal-linguist revision of the text.

ANNEX

COMPROMISE PROPOSAL

Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious ~~**transnational**~~ crime.

Recitals:

(1) On 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes. However, upon entry into force of the Treaty of Lisbon on 1 December 2009, the Commission's proposal, which had not been adopted by the Council by that date, became obsolete.

(2) The 'Stockholm Programme — An open and secure Europe serving and protecting the citizens'[1] 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 certain core elements of a Union policy in this area.

(4) Council Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data[2] regulates the transfer of advance passenger ~~information~~ data by air carriers to the competent national authorities for the purpose of improving border controls and combating ~~irregular~~ illegal immigration.

(4a) The objective of this Directive is, inter alia, to ensure security, to protect the life and safety of the citizens, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.

---

1 17024/09 CO EUR-PREP 3 JAI 896 POLGEN 229.

2 OJ L 261, 6.8.2004, p. 24.

(5) Effective use PNR data is ~~PNR data are~~ necessary to effectively prevent, detect, investigate and prosecute terrorist offences and [serious crime] and thus enhance internal security~~.~~ […], inter alia ~~(6) PNR data help law enforcement authorities prevent, detect, investigate and prosecute serious crimes, including acts of terrorism,~~by comparing ~~them~~ PNR data against ~~with~~ various databases o~~f~~n persons and objects sought, to construct evidence and, where relevant, to find associates of criminals and unravel criminal networks.

(6) […]

(7) The assessment of PNR data enables to identify persons who were ~~previously "unknown", i.e. persons~~ previously unsuspected of involvement in terrorism or serious crime ~~and terrorism~~ before an~~, but whom an~~ analysis of PNR ~~the~~ data suggests that they may be involved in such crime, and who should therefore be subject to further examination by the competent authorities. By using PNR ~~law enforcement authorities can~~ it is possible to address the threat of serious crime and terrorism from a different perspective than through the processing of other categories of personal data~~.~~ However, in order to ensure that the processing of data ~~of innocent and unsuspected persons~~ remains as limited as necessary ~~possible, the aspects of the use of PNR data relating to~~ the creation and application of assessment criteria should be ~~further~~ limited to ~~serious crimes that are also transnational in nature, i.e. are intrinsically linked to travelling and hence the type of the data being processed~~. terrorism and **specific** categories of serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria shall be defined in a manner which ensures that as few innocent people as possible are identified by the system.

(8) Air carriers already collect and process PNR data from their passengers for their own commercial purposes. This Directive should not impose any obligation on air carriers to collect or retain any additional data from passengers or to impose any obligation on passengers to provide any data in addition to that already being provided to air carriers.

(9) Some air carriers retain any collected advance passenger information (API) data as part of the PNR data, 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 and thus reinforcing the~~ir~~ law enforcement value of that result and minimising the risk of carrying out checks and investigations on persons non concerned. It is therefore important to ensure that, where air carriers collect API data, they should transfer it, irrespective of whether the API data is retained as part of the PNR data or not.

(10) In order ~~T~~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 ~~international flights to or from the territory of the Member States of the European Union~~ extra EU-flights, and if the Member State wishes to do so also on air carriers operating intra EU-flights, to transfer any collected PNR and API data. These provisions should be without prejudice to Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

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

(12) The definition of terrorist offences applied in this Directive should be ~~taken from Articles 1 to 4 of~~ the same as in Council Framework Decision 2002/475/JHA on combating terrorism[1]. The definition of [serious crime] should ***~~be taken from modelled on Article 2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedure between Member States., and should~~*** **encompass the categories of offence listed in Annex II to this Directive**[2]. ~~However, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality. The definition of serious transnational crime should be taken from Article 2 of Council Framework Decision 2002/584/JHA and the United Nations Convention on Transnational Organised Crime~~

[1] OJ L 164, 22.6.2002, p. 3.
[2] OJ L 190, 18.7.2002, p. 1.

(13) PNR data should be transferred to a single designated unit (Passenger Information Unit) in the relevant Member State, so as to ensure clarity and reduce costs to air carriers. The Passenger Information Unit may have different locations in one Member State and Member States may also jointly set up one Passenger Information Unit. **Members States should exchange the information among each other through relevant information exchange networks in order to facilitate information sharing and ensure interoperability between Member States**.

~~(13a) It is desirable that co-financing of the costs related to the establishment of the national~~ Passenger Information Units will be provided for under the instrument for financial support for police cooperation, preventing and combating crime, and crisis management as ~~part of the Internal Security Fund.~~ Member States should bear the costs of use, retention and exchange of PNR data.

(14) The contents of any lists of required PNR data to be obtained by ~~the~~ a Passenger Information Unit should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union as well as protecting the fundamental rights of ~~citizens~~ persons, notably privacy and the protection of personal data. **To that end, high standards 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') should be applied.** Such lists should not ~~contain any personal data that could reveal~~ be based on a person's race~~ial~~ or ethnic origin, religion or belief, political or any other opinion, ~~us or philosophical beliefs,~~ trade union membership, ~~or data concerning~~ health or sexual life ~~of the individual concerned~~ . The PNR data should contain **only** details on the passenger's reservation and travel itinerary which enable competent authorities to identify air passengers representing a threat to internal security.

(15) There are two possible methods of data transfer currently available: the 'pull' method, under which the competent authorities of the Member State requiring the data can reach into (access) the air carrier's reservation system and extract ('pull') a copy of the required data, and the 'push' method, under which air carriers transfer ('push') the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided. The 'push' method is considered to offer a higher degree of data protection and should be mandatory for all air carriers.

(16) The Commission supports the International Civil Aviation Organisation (ICAO) guidelines on PNR. These guidelines should thus be the basis for adopting the supported data formats for transfers of PNR data by air carriers to Member States. This justifies that such supported data formats, as well as the relevant protocols applicable to the transfer of data from air carriers should be adopted in accordance with the ~~advisory~~ examination procedure ~~foreseen~~ provided for in Regulation (EU) No. 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers[1].

(17) The Member States should take all necessary measures to enable air carriers to fulfil their obligations under this Directive. Dissuasive, effective and proportionate penalties, including financial ones, should be provided for by Member States against those air carriers failing to meet their obligations regarding the transfer of PNR data. ~~Where there are repeated serious infringements which might undermine the basic objectives of this Directive, these penalties may include, in exceptional cases, measures such as the immobilisation, seizure and confiscation of the means of transport, or the temporary suspension or withdrawal of the operating licence.~~

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

---

[1] OJ L 55, 28.02.2011, p. 13.

(19) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or seriously affects him/her should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Article**s 8 and** 21 of the Charter of Fundamental Rights of the European Union no such decision should ~~be taken by reason of~~ discriminate on any grounds such as a person's sex, race ~~or~~, colour, ethnic or social origin, ~~religious~~ genetic features, language, religion or ~~philosophical~~ belief, political or any other opinion, ~~trade union~~ membership~~, health~~ of a national minority, property, birth, disability, age or sexual orientation. These principles should also be taken into account when the Commission is reviewing the operation of this Directive.

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

(19b) Taking fully into consideration the principles of recent relevant case law outlined by the Court of Justice, the application of this Directive must ensure the full respect of fundamental rights and the right to privacy as well as the principle of proportionality. It must also genuinely meet the objectives of what is necessary and proportionate in order to achieve the general interests recognised by the Union and the need to protect the rights and freedoms of others in the fight against terrorism and serious crime. The application of this Directive must be duly justified and the necessary safeguards must be in place in order to ensure the lawfulness of any storage, analysis, transfer and use of PNR data.

(20) Member States should share with other Member States **and through Europol,** the PNR data that they receive where ~~such transfer~~ this is deemed necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime **Passenger Information Units should, where appropriate, without delay, transmit the result of the processing of PNR data to the Passenger Information Units 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 judicial authorities, including Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) and Council Framework Decision 2006/960/JHA of 18 September 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[1]. Such exchange of PNR data between law enforcement and judicial authorities should be governed by the rules on police and judicial cooperation **and should not undermine the high level of privacy and protection of personal data in accordance with the Charter, Convention No 108 and the ECHR**.

(20a) A secure exchange of information regarding PNR data should be assured between the Member States through any of the existing channels for cooperation between the competent authorities of the Member States, and with Europol through Europol's Secure Information Exchange Network Application (SIENA), in particular.

(21) The period during which PNR data are to be retained should be **necessary for, and** proportionate to the purposes of the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data are retained for a sufficiently long period for carrying out analysis and for use in investigations. In order to avoid disproportionate use, it is necessary that, after an initial period, the data are ~~anonymised~~ depersonalised through masking out and that the full PNR data are only accessible under very strict and limited conditions.

(21a) In order to ensure the highest level of data protection, access to the full PNR data set, which enables to immediately identify the data subject, should be granted only under very strict and limited conditions after the initial retention period.

---

1 OJ L 386, 29.12.2006, p. 89.

(22) Where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, the retention of such data by the competent authority should be regulated by the national law of the Member State, irrespective of the retention periods set ~~by~~ out in this Directive.

(23) The processing of PNR data domestically in each Member State by the Passenger Information Unit and by competent authorities should be subject to a standard of protection of personal data under their national law which is in line with **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 ~~('Framework Decision 2008/977/JHA')~~**, and the specific data protection requirements laid down in this Directive**. ***The references to Council Framework Decision 2002/977/JHA of 27 November 2008 should be understood as directing to the legislation currently in force as well as to future legislation that would replace it.***

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

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

(25a) This Directive allows the principle of public access to official documents to be taken into account.

(26) 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~~, the quality of the receiving authority and the safeguards applicable to the personal data transferred to the third country~~ **as well as to the principles of necessity and proportionality relating to the transfers, and to the high level of protection provided by the Charter, and the ECHR**

(27) The national supervisory authority that has been established in implementation of Framework Decision 2008/977/JHA should also be responsible for advising on and monitoring of the application ~~and implementation~~ of the provisions ~~of~~ adopted by the Member States pursuant to this Directive.

(28) This Directive does not affect the possibility for Member States to provide, under their domestic law, for a system of collection and ~~handling~~ processing of 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, ~~for purposes other than those specified in this Directive,~~ or from transportation providers other than those specified in the Directive~~, regarding internal flights subject to compliance with relevant data protection provisions~~, provided that such domestic law respects the Union acquis.~~ The issue of the collection of PNR data on internal flights should be the subject of specific reflection at a future date~~.

(28a) This Directive is without prejudice to the current Union rules on the way border controls are carried out or with the Union rules regulating entry and exit from the territory of the Union.

(29) 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, as well as the conditions under which this information needs to be provided to competent national authorities. These differences may be prejudicial to effective cooperation between the competent national authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

(30) Since the objectives of this Directive cannot be sufficiently achieved by the Member States, and can be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(31) This Directive respects the fundamental rights and the principles of the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof ~~the Charter~~ and has to be implemented accordingly. The Directive is compatible with data protection principles and its provisions are in line with the Framework Decision 2008/977/JHA. Furthermore, and in order to comply with the proportionality principle, the Directive, on specific issues, will have stricter rules on data protection than the Framework Decision 2008/977/JHA.

(32) In particular, the scope of ~~the~~ this Directive is as limited as possible, as it allows retention of PNR data in the Passenger Information Units for **a** period of time not exceeding ~~5~~ **five** years, after which the data ~~must~~ should be deleted, as the data ~~must~~ should be ~~anonymised~~ depersonalised through masking out after ~~a very short~~ an initial period, and as the collection and use of sensitive data ~~is~~ **should be** prohibited. In order to ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority **and, in particular, a data protection officer,** is responsible for advising and monitoring ~~how~~ the way PNR data are processed. All processing of PNR data ~~must~~ should be logged or documented for the purpose of verification of ~~the lawfulness of the data processing~~ its legality, self-monitoring and ensuring proper data integrity and security of the ~~data~~ processing. Member States ~~must~~ should also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.

(33) ~~[~~In accordance with Article 3 of the Protocol (No 21) on the position of United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, those Member States have notified their wish to participate in the adoption and application of this Directive~~]~~ ~~OR [Without prejudice to Article 4 of the Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, those Member States will not participate in the adoption of this Directive and will not be bound by or be subject to its application]~~.

(34) In accordance with Articles 1 and 2 of the Protocol (No 22) on the position of Denmark annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject-matter and scope

1. This Directive provides for the transfer by air carriers of Passenger Name Record data of passengers of ~~international~~ extra-EU flights to and from the Member States, as well as the processing of that data, ***including its collection, use and retention by the Member States and its exchange*** between ~~them.~~ **the Member States**.

2. The PNR data collected in accordance with this Directive may be processed only for the ~~following~~ purpose~~s~~ of~~:~~

   (a) ~~The~~ prevention, detection, investigation and prosecution of terrorist offences and serious crime ~~according to~~ as provided for in Article 4(2)(a), (b) and (c) ~~and~~

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

Article 1a

Application of the directive to intra-EU flights

1. If a Member State wishes to apply this Directive to intra-EU flights, it shall give notice in writing to the Commission to that end. The Commission shall publish such a notice in the Official Journal of the European Union. A Member State may give or revoke such notice at any time after the entry into force of this Directive.

2. Where such a notice is given, all the provisions of this Directive shall apply in relation to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if it 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 further the purposes of this Directive. The Member State may decide to change the selected~~ed~~ion of intra-EU flights at any time.

Article 2

Definitions

For the purposes of this Directive the following definitions apply:

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

(b) '~~international~~ extra-EU flight' means any scheduled or non-scheduled flight by an air carrier flying from a third country planned to land on the territory of a Member State ~~originating in a third country or to depart~~ or from the territory of a Member State ~~with a final destination~~ planned to land in a third country, including in both cases flights with any ~~transfer~~ stop-overs at the territory of Member States or ~~transit flights~~ third countries;

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

(c) ‘Passenger Name Record’ or 'PNR data' means a record of each passenger’s travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS, the system used to check passengers onto flights) or equivalent systems providing the same functionalities;

(d) ‘passenger’ means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, which is manifested by the persons’ registration in the passengers list and which includes transfer or transit passenger;

(e) ‘reservation systems’ means the air carrier’s internal ~~inventory~~ reservation system, in which PNR data are collected for the handling of reservations;

(f) ‘push method’ means the method whereby air carriers transfer **the required** PNR data **listed in Annex I** into the database of the authority requesting them;

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

~~(h) ‘serious crime’ means the offences under national law referred to in Article 2(2) of Council Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State, however, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality~~;

(i) ‘serious [..] crime’ means the offences, **listed in Annex II, where** ~~referred to in Article 2(2) of Council Framework Decision 2002/584/JHA if~~ they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State~~, and if~~;

~~(i) They are committed in more than one state;~~

~~(ii) They are committed in one state but a substantial part of their preparation, planning, direction or control takes place in another state;~~

~~(iii) They are committed in one state but involve an organised criminal group that engages in criminal activities in more than one state; or~~

~~(iv) They are committed in one state but have substantial effects in another state.~~

(j) 'depersonalising' through masking out of data' means rendering certain data elements of such data invisible to a user.

CHAPTER II

RESPONSIBILITES OF THE MEMBER STATES

Article 3

Passenger Information Unit

1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority**,** to act as its 'Passenger Information Unit' (PIU). **The PIU shall be** responsible for collecting PNR data from air carriers, ***for*** storing ~~them, analysing them~~, processing and transfer of those data or the result of the ~~analysis~~ processing thereof to the competent authorities referred to in Article 5. **The PIU shall also be responsible for the exchange of both PNR data and of the result of the processing thereof with the PIUs of other Member States and with Europol in accordance with Articles 7 and 7a.** Its staff members may be seconded from competent public authorities. Member States shall provide the PIUs with adequate resources in order to fulfil its tasks.

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

3. Each Member State shall notify the Commission thereof within one month of the establishment of the PIU and may at any time ~~update~~ ***modify*** its ~~declaration~~ notification. The Commission shall publish this ~~information~~ notification, including any ~~updates~~ modifications of it, in the Official Journal of the European Union.

Article 3a

Data Protection Officer in the Passenger Information Unit

1. The Passenger Information Unit shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing the related 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 the 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 the data subject's PNR data.

Article 4

Processing of PNR data

1. The PNR data transferred by the air carriers~~, pursuant to Article 6, in relation to international flights which land on or depart from the territory of each Member State~~ shall be collected by the Passenger Information Unit of the relevant Member State, as provided for by Article 6. Should the PNR data transferred by air carriers include data beyond those listed in ~~the~~ Annex I, the Passenger Information Unit shall delete such data immediately **and permanently** upon receipt.

2. The Passenger Information Unit shall process PNR data only for the following purposes:

   (a) carrying out an assessment of the passengers prior to their scheduled arrival to or departure from the Member State in order to identify ~~any~~ persons who ~~may be involved in a terrorist offence or serious transnational crime and who~~ require further examination by the competent authorities referred to in Article 5, **and, where relevant, by Europol, in accordance with Article 7a, in view of the fact that such persons may be involved in a terrorist offence or serious crime**.

(i) In carrying out such an assessment, the Passenger Information Unit may compare PNR data against ~~relevant~~ databases, relevant for the purpose of prevention, detection, investigation and prosecution of terrorist offences[and [serious crime], including ~~international or national~~ databases ~~or national mirrors of Union databases, where they are established on the basis of Union law~~, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such ~~files~~ databases.

(ii) When carrying out such an assessment ~~listed in Annex II to this Directive~~, the Passenger Information Unit may also process PNR data against pre-determined criteria.

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

(~~c~~b) responding, on a case-by-case basis, **subject** to a duly reasoned request~~s~~ **based on sufficient indication** from competent authorities to provide PNR data and to process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and to provide the competent authorities **or, where appropriate, Europol,** with the results of such processing; and

(c) analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments referred to in point (a)(ii) in order to identify any persons who may be involved in a terrorist offence or serious ~~transnational crime pursuant to point (a)~~ crime.

3. The assessment of the passengers prior to their scheduled arrival to or departure from the Member State carried out against pre-determined criteria referred to in point (a)(ii) of paragraph 2 shall be carried out in a non-discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. **These assessment criteria must be targeted, *proportionate* and specific.** Member States shall ensure that the assessment criteria are set by the Passenger Information Units in cooperation ***and regularly reviewed in cooperation*** with the competent authorities referred to in Article 5. The assessment criteria shall in no circumstances be based on a person's ~~race~~ racial or ethnic origin, political opinions, religion or philosophical beliefs, ~~political opinions,~~ trade union membership, health or sexual life.

4. The Passenger Information Unit of a Member State shall ~~transfer~~ transmit the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) ~~and (b)~~ of paragraph 2 for further examination to the ~~relevant~~ competent authorities referred to in Article 5 of the same Member State. Such transfers shall only be made on a case-by-case basis ***and in case of automated processing of PNR data*** **by non-automated means**.

4a. Member States shall ensure that the data protection officer has access to all data processed by the Passenger Information Unit. If the data protection officer considers that processing of any data was not lawful, he or she may refer the matter to the national supervisory authority.

4b. The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location within the territory of the Member States of the **European Union**.

5. The consequences of the assessments of passengers referred to in point (a) of paragraph 2 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. In addition, the consequences of such assessments, where these are carried out in relation to intra-EU flights between Member States to which the 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[1] applies, shall comply with that Code.

[1] OJ L 105, 13.4.2006, p.1.

Article 5

Competent authorities

1. Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of the processing of PNR data from the Passenger Information Units in order to examine that information further or to take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. **Europol shall be entitled to receive PNR data or the result of the processing of PNR data from the Passenger Information Units of the Member States within the limits of its competences and for the performance of its tasks.**

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

3. For the purpose of Article 7(4), e~~E~~ach Member State shall notify the list of its competent authorities to the Commission twelve months after entry into force of this Directive at the latest, and may at any time ~~update~~ modify ~~its declaration~~ this notification. The Commission shall publish this ~~information~~ notification, as well as any ~~updates~~ modifications of it, in the *Official Journal of the European Union*.

4. The PNR data ~~of passengers~~ and the result of the processing of PNR data received by the Passenger Information Unit may be further processed by the competent authorities of the Member States only for the **specific** purpose of prevention, detection, investigation or prosecution of terrorist offences **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**ial** or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health or sexual life

Article 6

Obligations on air carriers <u>on transfers of data</u>

1. Member States shall adopt the necessary measures to ensure that air carriers transfer ('push') the PNR data as defined in <u>point (c) of</u> Article 2~~(c)~~ and specified in ~~the~~ Annex <u>1</u>, to the extent that such data are already collected by them[<u>in the normal course of their business</u>, to the database of the ~~national~~ Passenger Information Unit of the Member State on the territory of which the ~~international~~ flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where ~~the~~ <u>an extra-EU flight</u> has one or more stop-overs at the airports of the Member States, air carriers shall transfer the PNR data <u>of all passengers</u> to the Passenger Information Units of all the Member States concerned. <u>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 intra-EU flight PNR data.</u>

<u>1a. In case the air carriers have collected any advance passenger information (API) data listed under item (18) of Annex 1 to this directive but do not retain these data as part of the PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer ('push') these data to the Passenger Information Unit of the Member State referred to in paragraph 1. In case of such transfer, all the provisions of this Directive shall apply in relation to these API data as if they were part of the PNR data.</u>

2. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the procedure ~~of~~ referred to in Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:

   (a) once 24 to 48 hours before the scheduled time for flight departure; and

   (b) once immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.

3. Member States ~~may~~ shall permit air carriers to limit the transfer referred to in point (b) of paragraph 2 to updates of the transfer referred to in point (a) of ~~paragraph 2~~ that paragraph.

4. On a case-by-case basis and 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 upon request from a Passenger Information Unit in accordance with national law, transfer PNR data ~~where access earlier~~ at other points in time than that mentioned in ~~point (a) of~~ paragraph 2 ~~is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime~~ (a) and (b).

Article 7

Exchange of information between Member States

1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2)(a) ~~and (b)~~, ***all relevant and necessary*** PNR data or the result of ~~the~~ any processing thereof ~~PNR data~~ is transmitted by that Passenger Information Unit to the ~~Passenger Information Units~~ corresponding units of ***the*** other Member States ~~where the former Passenger Information Unit~~ it ~~considers such transfer to be necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious~~ crime. The Passenger Information Units of the receiving Member States shall transmit ~~such PNR data or the result of the processing of PNR data~~ the received information to their ~~relevant~~ competent authorities in accordance with Article 4(4).

2. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database ~~in accordance with~~ and have not yet been depersonalised through masking out under Article 9(~~1~~2), and, if necessary, also the result of ~~the~~ any processing ~~of PNR data~~ thereof, if it has already been prepared pursuant to Article 4(2)(a). The duly reasoned request for such data may be based on any one or a combination of data elements, as deemed necessary by the requesting Passenger Information Unit for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime. Passenger Information Units shall provide the requested data as soon as practicable ~~and shall provide also the result of the processing of PNR data, if it has already been prepared pursuant to Article 4(2)(a) and (b)~~. In case the requested data have been depersonalised through masking out in accordance with Article 9(2) the Passenger Information Unit shall only provide the full PNR data where it is reasonably believed that it is necessary for the purpose of Article 4(2)(b) and only when authorised to do so by an authority competent under Article 9(3).

~~3. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(2), and, if necessary, also the result of the processing of PNR data. The Passenger Information Unit may request access to specific PNR data kept by the Passenger Information Unit of another Member State in their full form without the masking out only in exceptional circumstances in response to a specific threat or a specific investigation or prosecution related to terrorist offences or serious crime.~~

4. Only when necessary in cases of emergency and under the conditions laid down in paragraph 2 ~~in those cases where it is necessary for the prevention of an immediate and serious threat to public security~~ may the competent authorities of a Member State request directly the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database ~~in accordance with Article 9(1) and (2)~~. The requests from the competent authorities, a copy of which shall always be sent to the Passenger Information Unit of the requesting Member State ~~Such requests shall relate to a specific investigation or prosecution of terrorist offences or serious crime and~~ shall be reasoned. ~~Passenger Information Units shall respond to such requests as a matter of priority.~~ In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.

5. Exceptionally, where ~~early~~ access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the Passenger Information Unit of a Member State shall at any time have the right to request the Passenger Information Unit of another Member State to ~~provide it with~~ obtain PNR data ~~of flights landing~~ in accordance with article 6(4) and provide it to the requesting Passenger Information Unit ~~or departing from the latter's territory at any time~~. ***(…)***

6. Exchange of information under this Article may take place using any existing channels for ~~international law enforcement~~ cooperation between the competent authorities of the Member States**,** [in particular Europol, the Secure Information Exchange Network Application (SIENA) and national units established in accordance with Article 8 of Decision 2009/371/JHA]. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contact~~s~~ points to which requests may be sent in cases of ~~urgency~~ emergency. The Commission shall communicate to the Member States the notifications received.

Article 7a

Conditions for access to PNR data by Europol

1. Europol may submit, on a case-by-case basis, an electronic and duly reasoned request to the Passenger Information Unit of any Member State through the Europol National Unit for the transmission of specific PNR data or the results of the processing of specific PNR data, when this is strictly necessary to support and strengthen action by Member States 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. The reasoned request shall set out reasonable grounds on the basis of which Europol considers that the transmission of PNR data or the results of the processing of PNR data will substantially contribute to the prevention, detection, investigation or prosecution of the criminal offence concerned.

2. 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.

3. 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 8

Transfer of data to third States

1. A Member State may transfer PNR data ~~and~~ as well as the results of the processing of ~~PNR~~ such data stored by the Passenger Information Unit in accordance with Article 9 to a third country, only on a case-by-case basis and if:

(a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled;

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

(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 specified in Article 1(2) and only with the express authorisation of the Member State.;

(d) similar ***same*** conditions as those laid down in Article 7(2) are fulfilled.

In exceptional circumstances, transfers of PNR data without prior consent shall be permitted only if such transfers are essential to respond to a specific and actual threat related to terrorist offences or serious crime of a Member State or a third country ***(…)*** and 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.

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

(…)

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

Article 9

Period of data retention

1. Member States shall ensure that the PNR data provided by the air carriers to the Passenger Information Unit are retained in a database at the Passenger Information Unit for a period of 30 days five years after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.

2. Upon expiry of ~~the~~a period of ~~30 days~~ ***[6] months*** after the transfer of the PNR data ~~to the Passenger Information Unit~~as referred to in paragraph 1, ***(…)*** all PNR data shall be depersonalised through masking out the following data elements which could serve to directly identify the passenger to whom the PNR data relate ~~shall be masked out. Such anonymised PNR data shall be accessible only to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria according to Article 4(2)(d). Access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit for the purposes of Article 4(2)(c) and where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution.~~

~~For the purposes of this Directive, the data elements which could serve to identify the passenger to whom PNR data relate and which should be filtered and masked out are~~:

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

2. Address and contact information;

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

4. Frequent flyer information;

5. General remarks to the extent that it contains any information which could serve to directly identify the passenger to whom the PNR relate; and

6. Any collected ~~A~~advance ~~P~~passenger ~~I~~information.

3. Upon expiry of the ***[6] months*** period referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is reasonably believed that it is necessary for the purpose of Article 4(2)(b).

Disclosure of the full PNR data can be permitted only when approved :

- by a judicial authority or,

- by another national authority competent under national law to verify whether the conditions for disclosure are fulfilled, ***subject to information and ex post review by the data protection officer of the Passenger Information Unit***,

~~3~~4. Member States shall ensure that the PNR data are deleted **permanently** upon expiry of the period specified in paragraph 2. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific ~~criminal investigations~~ case for the purpose of prevention, detection, investigation or prosecution~~s~~, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.

~~4~~5. The result of ~~matching~~the processing referred to in Article 4(2)(a) ~~and (b)~~ shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities and, according to Article 7(1) the Passenger Information Units of other Member States of a positive match. Where the result of an automated ~~matching operation~~processing has, further to individual review by non-automated means as referred to in Article 4(2)(a) last subparagraph, proven to be negative, it ~~shall~~may, however, be stored so as to avoid future 'false' positive matches for ~~a maximum period of three years unless~~as long as the underlying data have not yet been deleted in accordance with ***Article 4*** ~~at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted~~.

Article 10

Penalties against air carriers

Member States shall ensure, in conformity with their national law, that dissuasive, effective and proportionate penalties, including financial penalties, are provided for against air carriers which, do not transmit the data ~~required under this Directive, to the extent that they are already collected by the them,~~ as provided for in Article 6, or do not do so in the required format or otherwise infringe the national provisions adopted pursuant to this Directive.

Article 11

Protection of personal data

1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data**,** right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as ~~those adopted under~~ laid out in national and Union law**,** and in the implementi~~n~~gation of Articles 17, 18, 19 and 20 of the Framework Decision 2008/977/JHA. Those Articles shall therefore be applicable.

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

2a. This Directive is without prejudice to the applicability of Directive 95/46 to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organizational measures to protect the security and confidentialty of personal data.

3. Member States shall prohibit ~~Any~~ the processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, ***(…)*** health or sexual life ***or sexual orientation***. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately.

3a. Member States shall ensure that the Passenger Information Unit maintains documentation of 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 Passenger Information Unit entrusted with the processing of the PNR data, the different levels of access authorisation and the personnel concerned;

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

(c) all requests and transfers of data to a third country.

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

3b. Member States shall ensure that the Passenger Information Unit keeps records of at least the following processing operations: collection, consultation, disclosure or erasure. The records of consultation and disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed the PNR data, and the identity and recipients of that data. The records shall be used solely for the purposes of verification, self-monitoring and for ensuring data integrity and data security or for purposes of auditing. The Passenger Information Unit shall make the records available, on request, to the national supervisory authority.

The records shall be kept for a period of five years**.**

3c. Member States shall ensure that their Passenger Information Unit implements appropriate technical and organisational measures and procedures to ensure a high level of security appropriate to the risks represented by the processing and the nature of the PNR data to be protected.

3d. Member States shall ensure that where a personal data breach is likely to result in a high risk the protection of the personal data or the privacy of the data subject adversely, the Passenger Information Unit shall communicate that breach to the data subject and to the national data protection supervisor without undue delay.

[…]

7. Without prejudice to Article 10, Member States shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Directive.

Article 12

National supervisory authority

Each Member State shall provide that the national supervisory authority ***(…)*** ~~established in~~ to implement~~ation of~~ 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. The further provisions of Article 25 Framework Decision 2008/977/JHA shall be applicable.

Article 12a

Duties and powers of the national supervisory authority

1. The national supervisory authority of each Member State shall be responsible for monitoring the application of the provisions adopted pursuant to this Directive with a view to protect fundamental rights in relation to the processing of personal data. Each national supervisory authority shall:

(a) hear 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) **check the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint, and inform the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable time period;**

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

CHAPTER III ~~IV~~

IMPLEMENTING MEASURES

Article 13

Common protocols and supported data formats

1. All transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made by electronic means ~~or~~, which provide sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. I~~i~~n the event of technical failure, the PNR data shall be transferred by any other appropriate means, for a period of one year following the adoption of the common protocols and supported data formats in accordance with Article 14 whilst maintaining the same level of security and in full compliance with Union data protection law.

2. Once the period of one year from the date of adoption, for the first time, of the common protocols and supported data formats by the Commission in accordance with paragraph 3, has elapsed, all transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of those accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.

3. The list of accepted common protocols and supported data formats shall be drawn up and, if need be, adjusted, by the Commission in accordance with the by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 14(2).

4. As long as the accepted common protocols and supported data formats referred to in paragraphs 2 and 3 are not available, paragraph 1 shall remain applicable.

5. Each Member State shall ensure that the necessary technical measures are adopted to be able to use the common protocols and data formats within one year from the date the common protocols and supported data formats ~~are adopted~~ referred to in paragraph 2.

Article 14

Committee procedure

1. The Commission shall be assisted by a committee ~~('the Committee')~~. That Committee shall be a committee within the meaning of Regulation ~~[…~~(EU) No. 82/2011~~/EU] of 16 February 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. The Commission shall not adopt the draft implementing act when no opinion is delivered by the Committee and the third subparagraph of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

2. Where reference is made to this paragraph, Article ***4*** of Regulation ~~[…/2011/~~EU~~] of 16 February~~No. 182/2011 shall apply.

CHAPTER IV

FINAL PROVISIONS

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest two years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions.

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

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

~~Article 16~~

~~Transitional provisions~~

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

Article 17

Review

1. On the basis of these discussions as well as other information provided by the Member States, **including the statistical information referred to in Article 18(2),** ~~the Commission shall~~

   ~~(a) review the feasibility and necessity of including internal flights in the scope of this Directive, in the light of the experience gained by those Member States that collect PNR data with regard to internal flights. T~~the Commission shall by …*[two years after the date of transposition referred to in Article 15(1)], conduct a review of the operation of this Directive and submit a report to the European Parliament and to the Council.~~within two years after the date mentioned in Article 15(1);~~

   ~~(b) undertake a review of the operation of this Directive and submit a report to the European Parliament and the Council within four years after the date mentioned in Article 15(1). Such review shall cover all the elements of this Directive, with special attention to the compliance with standard of protection of personal data, In conducting its review, the Commission shall pay special attention to compliance with the standards of protection of personal data, the necessity and proportionality of the collection and processing of PNR data for each of the stated purposes, the length of the data retention period and the quality of the assessments and the effectiveness of the sharing of data between the Member States, and the quality of the assessment including with regard to the statistical information gathered pursuant to Article 18.

   The report submitted shall also include a review on the feasibility and necessity of including all or selected intra-EU flights in the scope of this Directive on a mandatory basis, taking into account the experience gained by Member States, especially those Member States that in accordance with Article 1a collect PNR with regard to intra-EU flights. ***The report shall also look at the necessity of introducing non carrier economic operators within the scope of this Directive.***

   (…)

2. If appropriate, in light of the review referred to in paragraph 2, the Commission shall make a legislative proposal to the European Parliament and the Council with a view to amending this Directive.

Article 18

Statistical data

1. Member States shall ~~prepare~~ provide on a yearly basis the Commission with a set of statistical information on PNR data provided to the Passenger Information Units. ~~Such~~ These statistics shall not contain any personal data.

2. The statistics shall as a minimum cover the

   (a) total number of ~~identifications of any persons who may be involved in a terrorist offence or serious crime according to Article 4(2)~~ passengers whose PNR data were collected and exchanged;

   (b) number of passengers identified for further scrutiny;

   (c) ~~and the~~ number of subsequent law enforcement actions that were taken involving the use of PNR data ~~per air carrier and destination.~~

Article 19

Relationship to other instruments

1. Member States may continue to apply bilateral or multilateral agreements or arrangements between themselves on exchange of information between competent authorities, in force when this Directive is adopted, in so far as such agreements or arrangements are compatible with this Directive.

1a. This Directive is without prejudice to the applicability of Directive 95/46 to the processing of personal data by air carriers.

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

Article 20

Entry into force

This Directive shall enter into force the twentieth day following that of its publication in the *Official Journal of the European Union.*

This Directive is addressed to the Member States in accordance with the Treaties.

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 PNR

(18) Any Advance Passenger Information (API) data collected (inter alia document type, document number, nationality, country of issuance, date of document expiration, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time, arrival time)

(19) All historical changes to the PNR listed in numbers 1 to 18.

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 EU,
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.