

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 crime	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 crime	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		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
--	--	---	--	---

Article 1

Subject-matter and scope	Subject-matter and scope	Subject-matter and scope		Subject-matter and scope
1. This Directive provides for the transfer by air carriers of Passenger Name Record data of passengers of international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by the Member States and its exchange between them.	1. This Directive provides for the transfer by air carriers of Passenger Name Record (PNR) data of passengers of international <u>extra-EU</u> 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.	1. This Directive provides for the transfer by air carriers and non-carrier economic operators of Passenger Name Record data of passengers of international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by the Member States and its exchange between the Member States and between the Member States and Europol.		1. This Directive provides for the transfer by air carriers and non-carrier economic operators of Passenger Name Record data of passengers of <u>extra EU</u> 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 the Member States and between the Member States and Europol.

<p>2. The PNR data collected in accordance with this Directive may be processed only for the following purposes:</p> <p>(a) The prevention, detection, investigation and prosecution of terrorist offences and serious crime according to Article 4(2)(b) and (c); and</p> <p>(b) The prevention, detection, investigation and prosecution of terrorist offences and serious transnational crime according to Article 4(2)(a) and (d).</p>	<p>2. The PNR data collected in accordance with this Directive may be processed only for the following purposes:</p> <p>(a) The prevention, detection, investigation and prosecution of terrorist offences and serious crime according to as provided for Article 4(2)(a), (b) and (c); and</p> <p>(b) The prevention, detection, investigation and prosecution of terrorist offences and serious transnational crime according to Article 4(2)(a) and (d).</p>	<p>2. The PNR data collected in accordance with this Directive may be processed only for the purposes of the prevention, detection, investigation and prosecution of terrorist offences and of certain types of serious transnational crime in accordance with Article 4(2) or the prevention of an immediate and serious threat to public security.</p>		<p>2. The PNR data collected in accordance with this Directive may be processed only for the purposes of the prevention, detection, investigation and prosecution of terrorist offences and of certain types of serious transnational crime in accordance with Article 4(2) or the prevention of an immediate and serious threat to public security.</p>
Article 1a				
	Application of the directive to intra-EU flights			
	<p><u>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</u></p>			<p><u>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</u></p>

	<u>Directive.</u>			<u>or revoke such notice at any time after the entry into force of this Directive.</u>
	<u>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.</u>			<u>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.</u>
	<u>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 intra-EU flights at any time.</u>			<u>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 intra-EU flights at any time.</u>

Article 2				
Definitions	Definitions	Definitions		Definitions

For the purposes of this Directive the following definitions shall apply:	For the purposes of this Directive the following definitions shall apply:	For the purposes of this Directive the following definitions apply:		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;	(a) 'air carrier' means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage by air of passengers;	(a) 'air carrier' means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage by air of passengers;		(a) 'air carrier' means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage by air of passengers;
		(aa) 'non-carrier economic operator' means an economic operator, such as travel agencies and tour operators, which provides travel-related services, including the booking of flights for which they collect and process PNR data of passengers;		(aa) 'non-carrier economic operator' means an economic operator, such as travel agencies and tour operators, which provides travel-related services, including the booking of flights for which they collect and process PNR data of passengers; <i>Proposal: Move to recital in conjuncture with including this in the review mechanism</i>
(b) 'international flight' means any scheduled or non-scheduled flight by an air carrier planned to land on the territory of a Member State originating in a third country or to depart from the territory of	(b) 'international—extra-EU flight' means any scheduled or non-scheduled flight by an air carrier <u>flying from a third country</u> planned to land on the territory of a Member State originating in a third country or to depart or	(b) 'international flight' means any scheduled or non-scheduled flight by an air carrier planned to land on the territory of a Member State originating in a third country or to depart from the territory of a Member State with a		(b) '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 or from the territory of

<p>a Member State with a final destination in a third country, including in both cases any transfer or transit flights;</p>	<p>from the territory of a Member State with a final destination <u>planned to land in a third country, including in both cases <u>flights with any transfer stop-overs at the territory of Member States or transit flights</u> third countries;</u></p>	<p>final destination in a third country, including in both cases any transfer or transit flights;</p>		<p>a Member State planned to land in a third country, including in both cases flights with any stop-overs at the territory of Member States or third countries;</p>
	<p><u>(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;</u></p>			<p>(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;</p>
<p>(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</p>	<p>(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</p>	<p>(c) ‘Passenger Name Record’ or ‘PNR data’ means a record of each passenger’s travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS) or equivalent systems providing the same</p>		<p>(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</p>

Systems (DCS) or equivalent systems providing the same functionalities;	any person, whether it is contained in reservation systems, Departure Control Systems (DCS) , <u>the system used to check passengers onto flights</u>) or equivalent systems providing the same functionalities;	functionalities;		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 carrier;	(d) ‘passenger’ means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the <u>air carrier, which is manifested by the persons’ registration in the passengers list and which includes transfer or transit passenger</u> ;	(d) ‘passenger’ means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the carrier;		(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 system, in which PNR data are collected for the handling of reservations;	(e) ‘reservation systems’ means the air carrier’s internal inventory <u>reservation</u> system, in which PNR data are collected for the handling of reservations;	(e) ‘reservation systems’ means the air carrier’s or non-carrier economic operator’s internal inventory system, in which PNR data are collected for the handling of reservations;		(e) ‘reservation systems’ means the air carrier’s {or, where applicable, non-carrier economic operator’s} internal 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 into the database of the authority	(f) ‘push method’ means the method whereby air carriers transfer the required PNR data into the database of the authority requesting	(f) ‘push method’ means the method whereby air carriers or non-carrier economic operators transfer the required PNR data listed in the Annex into the database		(f) ‘push method’ means the method whereby air carriers {or, where applicable, non-carrier economic operators} transfer the required PNR

requesting them;	them;	of the authority requesting them;		data listed in <i>the Annex I</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 Council Framework Decision 2002/475/JHA;	(g) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;	(g) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;		(g) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;

<p>(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;</p>	<p>(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;</p>	<p>(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;</p>		
<p>(i) ‘serious transnational 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</p>	<p>(i) ‘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</p>	<p>(i) ‘serious transnational crime’ means the following offences, where 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</p>	<p>List of offences to be agreed upon with EP, see Annex. Offences added to reflect the EP proposed amendments.</p>	<p>(i) ‘serious crime’ means the offences listed in Annex II, where they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the</p>

<p>detention order for a maximum period of at least three years under the national law of a Member State, and if :</p> <p>(i) They are committed in more than one state;</p> <p>(ii) They are committed in one state but a substantial part of their preparation, planning, direction or control takes place in another state;</p> <p>(iii) They are committed in one state but involve an organised criminal group that engages in criminal activities in more than one state; or</p> <p>(iv) They are committed in one state but have substantial effects in another state.</p>	<p>sentence or a detention order for a maximum period of at least three years under the national law of a Member State, and if :</p> <p>(i) They are committed in more than one state;</p> <p>(ii) They are committed in one state but a substantial part of their preparation, planning, direction or control takes place in another state;</p> <p>(iii) They are committed in one state but involve an organised criminal group that engages in criminal activities in more than one state; or</p> <p>(iv) They are committed in one state but have substantial effects in another state.</p>	<p>State, as referred to in Article 2(2) of Council Framework Decision 2002/584/JHA;</p> <ul style="list-style-type: none"> - participation in a criminal organisation, - trafficking in human beings, facilitation of unauthorised entry and residence, illicit trade in human organs and tissue, - sexual exploitation of children and child pornography, rape, female genital mutilation, - illicit trafficking in narcotic drugs and psychotropic substances, - illicit trafficking in weapons, munitions and explosives, - serious fraud, fraud against the financial interests of the EU, laundering of the proceeds of crime, money laundering and counterfeiting currency, - murder, grievous bodily 		<p>national law of a Member State, as referred to in Article 2(2) of Council Framework Decision 2002/584/JHA</p>
---	---	---	--	---

		<p>injured, kidnapping, illegal restraint and hostage-taking, armed robbery,</p> <ul style="list-style-type: none">- serious computer-related crime and cybercrime,- environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,- forgery of administrative documents and trafficking therein, illicit trafficking in cultural goods, including antiques and works of art, counterfeiting and piracy of products,- unlawful seizure of aircraft/ships,- espionage and treason,- illicit trade and trafficking in nuclear or radioactive materials and their precursor and in this regard non-proliferation related crimes,- crimes within the		
--	--	--	--	--

		jurisdiction of the International Criminal Court.		
	(j) <u>'depersonalising through masking out of data' means rendering certain data elements of such data invisible to a user</u>			(j) 'depersonalising through masking out of data' means rendering certain data elements of such data invisible to a user.

CHAPTER II

RESPONSIBILITIES OF THE MEMBER STATES

Article 3

Passenger Information Unit	Passenger Information Unit	Passenger Information Unit	Passenger Information Unit
<p>1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime or a branch of such an authority to act as its 'Passenger Information Unit' responsible for collecting PNR data from the air carriers, storing them, analysing them and transmitting the result of the analysis to the competent authorities referred to in Article 5. Its staff members may be seconded from competent public authorities.</p>	<p>1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime or a branch of such an authority to act as its 'Passenger Information Unit' (PIU) responsible for collecting PNR data from the air carriers, storing them, analysing <u>processing</u> them and transmitting the <u>PNR data or the result of the analysis processing thereof</u> to the competent authorities referred to in Article 5. <u>The PIU is also responsible for the exchange of PNR data or the result of the processing thereof with PIUs of other Member States in accordance with Article 7.</u> Its staff members may be seconded from competent public authorities. <u>It shall be</u></p>	<p>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 transnational crime and for the prevention of immediate and serious threats to public security, or a branch of such an authority, to act as its 'Passenger Information Unit'. The Passenger Information Unit shall be responsible for collecting PNR data from air carriers and non-carrier economic operators, storing, processing and analysing those data and transmitting the result of the analysis to the competent authorities referred to in Article 5. The Passenger Information Unit shall also be responsible for the exchange of PNR data and of the result of the processing thereof with the Passenger</p>	<p>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 storing, processing and transmitting those data or the result of the processing thereof to the competent authorities referred to in Article 5. The PIU shall also be responsible for the exchange of PNR data and of the result of the processing thereof with the PIUs of other Member States and</p>

	<p><u>provided with adequate resources in order to fulfil its task.</u></p>	<p>Information Units of other Member States and with Europol in accordance with Articles 7 and 7a, and for conducting the assessments referred to in Article 4. Its staff members may be seconded from competent public authorities. Member States shall provide the Passenger Information Unit with adequate resources in order to fulfil its tasks.</p>		<p>with Europol in accordance with Articles 7 and 7a, and for conducting the assessments referred to in Article 4. 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.</p>
<p>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 on the detailed rules for the operation of the Passenger Information Unit and shall respect the requirements laid down in this Directive.</p>	<p>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 on the detailed rules for the operation of the Passenger Information Unit and shall respect the requirements laid down in this Directive.</p>	<p>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.</p>		<p>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</p>

				in this Directive.
3. Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and may at any time update its declaration. The Commission shall publish this information, including any updates, in the Official Journal of the European Union.	3. Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and thereof . It may at any time update <u>modify its declaration</u> notification . The Commission shall publish this information, including any updates <u>modifications</u> of it, in the Official Journal of the European Union.	3. Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and shall at any time update its declaration. The Commission shall publish this information, including any updates, in the Official Journal of the European Union.		3. Each Member State shall notify the Commission thereof within one month of the establishment of the PIU and shall at any time update its notification. The Commission shall publish this information, including any modifications, in the Official Journal of the European Union.

Article 3a				
		Data Protection Officer in the Passenger Information Unit:		
		<p>1. All staff members of the Passenger Information Unit who have access to PNR data shall receive specifically tailored training on processing of PNR data in full compliance with data protection principles and fundamental rights.</p> <p>2. The Passenger Information Unit shall appoint a data protection officer responsible for</p>		<p><i>1: The Passenger Information Unit shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing the related safeguards.</i></p> <p><i>2: Member States shall provide data protection officers with the means to perform their duties</i></p>

		<p>monitoring the processing of PNR data and implementing the related safeguards.</p> <p>3. Member States shall ensure that the data protection officer is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in this Directive. Member States shall provide that any other professional duties of the data protection officer are compatible with that person's tasks and duties as data protection officer and do not result in a conflict of interest. The data protection officer shall:</p> <p>(a) raise awareness and advise staff members of the Passenger Information Unit regarding their obligations concerning the protection of personal data, including the training of staff members and the assignment of responsibilities;</p> <p>(b) monitor the implementation and application of data protection requirements laid</p>	<p><i>and tasks in accordance with this Article effectively and independently.</i></p> <p><i>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.</i></p> <p><i>(Could include within Article 3)</i></p>
--	--	--	--

		<p>down in this Directive, in particular through conducting random sampling of data processing operations;</p> <p>(c) ensure that all documentation is maintained and records kept in accordance with this Directive, and monitor documentation, notification and communication of personal data breaches and report wrongful conduct as regards the data protection requirements laid down in this Directive to the appropriate authorities;</p> <p>(d) monitor responses to requests from the national supervisory authority and cooperate with the national supervisory authority, especially on matters relating to data transfers to other Member States or to third countries, and act as contact point for the national supervisory authority on issues related to the processing of PNR data, where appropriate, contacting the national supervisory authority on his or her own initiative.</p>		
--	--	--	--	--

		<p>Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently.</p> <p>4. 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. Member States shall ensure that the name and contact details of the data protection officer are communicated to the national supervisory authority and to the public.</p>		
--	--	---	--	--

Article 4				
Processing of PNR data	Processing of PNR data	Processing of PNR data		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	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	1. The PNR data transferred by the air carriers and the non-carrier economic operators , pursuant to Article 6, in relation to international flights which land on or depart from the territory of <i>a</i> Member State shall be collected by the Passenger Information Unit of the		1. The PNR data transferred by the air carriers 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

relevant Member State. Should the PNR data transferred by air carriers include data beyond those listed in the Annex, the Passenger Information Unit shall delete such data immediately upon receipt.	relevant Member State, <u>as provided for Article 6</u> . Should the PNR data transferred by air carriers include data beyond those listed in the Annex, the Passenger Information Unit shall delete such data immediately upon receipt.	that Member State. Should the PNR data transferred by air carriers and non-carrier economic operators include data beyond those listed in the Annex, the Passenger Information Unit shall delete such data immediately and permanently upon receipt.		include data beyond those listed in Annex, the Passenger Information Unit shall delete such data immediately and permanently upon receipt. ⁰
2. The Passenger Information Unit shall process PNR data only for the following purposes:	2. The Passenger Information Unit shall process PNR data only for the following purposes:	2. The Passenger Information Unit shall process PNR data only for the following purposes:		2. The Passenger Information Unit shall process PNR data only for the following purposes:
(a) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious transnational crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment, the Passenger Information Unit may process PNR data against pre-determined criteria. Member States shall ensure that any positive match resulting from such automated processing is	(a) carrying out an assessment of the passengers prior to their scheduled arrival <u>to</u> or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious transnational crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment, the Passenger Information Unit may process PNR data against pre-determined criteria. Member States shall ensure that any positive match resulting from such automated processing is	(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 carrying out such an assessment, the Passenger Information Unit may process PNR data against pre-determined criteria in accordance with this Directive, and may compare PNR data against relevant	Check language from recital (5): (5) PNR data are necessary to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, inter alia by comparing them with various databases of persons and objects sought, to construct evidence and, where relevant, to find associates of criminals and unravel criminal networks.	(a) carrying out an assessment of the passengers prior to their scheduled arrival to or departure from the Member State in order to identify persons 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]/criminal networks.

<p>individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;</p>	<p>individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;</p>	<p>databases, including international or national databases or national mirrors of Union databases, where they are established in compliance with Union law, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such files, in accordance with the requirements set out in paragraph 3. Member States shall ensure that any positive match resulting from such automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;</p>		<p>(i) In carrying out such an assessment the Passenger Information Unit may compare PNR data against databases, relevant for the purpose of prevention, detection, investigation and prosecution of terrorist offences [and serious crime], including databases, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases.</p> <p>(ii) When carrying out an assessment of persons who may be involved in [a terrorist offence or serious crime] listed in Annex II to this Directive, the Passenger Information Unit may also process PNR data against pre-determined criteria.</p> <p>Member States shall ensure that any positive match resulting from automated processing of</p>
---	--	---	--	---

				<p>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;</p>
<p>(b) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment the Passenger Information Unit may compare PNR data against relevant databases, 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</p>	<p>(b) — carrying out an assessment in view of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any fact that such persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities referred to in Article 5.</p> <p><u>(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</u></p>	<p>(b) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious transnational crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment the Passenger Information Unit may compare PNR data against relevant databases, including national databases or national mirrors of Union databases, on persons or objects sought or under alert, in accordance with Union and national rules applicable to such databases for the purpose of preventing, detecting,</p>		

<p>with Union, international and national rules applicable to such files. Member States shall ensure that any positive match resulting from such automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;</p>	<p>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.</p> <p><u>(ii) When carrying out an assessment of persons who may be involved in a terrorist offence or serious crime listed in Annex II to this Directive, the Passenger Information Unit may also process PNR data against pre-determined criteria.</u></p> <p>Member States shall ensure that any positive match resulting from such automated processing of PNR data <u>conducted under point (a) of paragraph 2</u> is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action <u>in accordance with national law;</u></p>	<p>investigating and prosecuting terrorist offences and serious transnational crime. In carrying out such an assessment, the Passenger Information Unit may compare PNR data against the Schengen Information System and the Visa Information System. Member States shall ensure that any positive match resulting from such automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;</p>		
<p>(c) responding, on a case-by-case basis, to duly reasoned requests from</p>	<p>(b) responding, on a case-by-case basis, to duly reasoned requests from competent</p>	<p>(c) responding, on a case-by-case basis based on sufficient evidence, to duly reasoned</p>		<p>(b) responding, on a case-by-case basis, subject to a duly</p>

<p>competent authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and to provide the competent authorities with the results of such processing; and</p>	<p>authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and to provide the competent authorities with the results of such processing; and</p>	<p>requests from competent authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or of serious transnational crime listed in point (i) of Article 2 or for the prevention of an immediate and serious threat to public security, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and</p>		<p>reasoned requests based on sufficient indication from competent authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime {or for the prevention of an immediate and serious threat to public security}, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and</p>
<p>(d) analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify any persons who may be involved in a terrorist offence or serious transnational crime pursuant to point (a).</p>	<p>© analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments <u>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) crimes listed in Annex II.</u></p>	<p>(d) analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify any persons who may be involved in a terrorist offence or serious transnational crime pursuant to point (a).</p>		<p>(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 crimes listed in Annex II.</p>
<p>3. The assessment of the passengers prior to their</p>	<p>3. The assessment of the passengers prior to their</p>	<p>3. The assessment of the passengers prior to their</p>		<p>3. The assessment of the passengers prior to</p>

<p>scheduled arrival or departure from the Member State referred to in point (a) of paragraph 2 shall be carried out in a non-discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities referred to in Article 5. The assessment criteria shall in no circumstances be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.</p>	<p>scheduled arrival or departure from the Member State <u>carried out against pre-determined criteria</u> referred to in point (a) of paragraph 2 shall be carried out in a non-discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities referred to in Article 5. The assessment criteria shall in no circumstances be based on a person's race <u>racial</u> or ethnic origin, <u>political opinions</u>, religious or philosophical beliefs, political opinion, trade union membership, health or sexual life.</p>	<p>scheduled arrival or departure from the Member State referred to in point (a) of paragraph 2 shall be carried out in a non-discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. This assessment criteria must be targeted, specific, justified, proportionate and fact-based. A regular review shall involve the data protection officer; Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities referred to in Article 5 and regularly reviewed. The assessment criteria shall in no circumstances be based on person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sexual life;</p>		<p>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 with the competent authorities referred to in Article 5 and regularly reviewed. The assessment criteria shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership and the processing of data concerning health or sexual life.</p>
---	--	---	--	--

<p>4. The Passenger Information Unit of a Member State shall transfer the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) and (b) of paragraph 2 for further examination to the relevant competent authorities of the same Member State. Such transfers shall only be made on a case-by-case basis.</p>	<p>4. The Passenger Information Unit of a Member State shall transfer <u>transmit</u> the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) and (b) of paragraph 2 for further examination to the relevant competent authorities of the same Member State <u>referred to in Article 5</u>. Such transfers shall only be made on a case-by-case basis.</p>	<p>4. The Passenger Information Unit of a Member State shall transfer the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) and (b) of paragraph 2 for further examination to the relevant competent authorities of the same Member State. Such transfers shall only be made on a case-by-case basis by human action.</p>		<p>4. The Passenger Information Unit of a Member State shall transmit the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) of paragraph 2 for further examination to the competent authorities of the same Member State referred to in Article 5. Such transfers shall only be made on a case-by-case basis by non automated means.</p>
		<p>4a. Member States shall ensure that the data protection officer has access to all data transmitted to the Passenger Information Unit and from the Passenger Information Unit to a competent authority pursuant to Article 5. If the data protection officer considers that transmission of any data was not lawful, he or she shall refer the matter to the national supervisory authority, which shall have power to order the receiving competent authority to delete that data.</p>		<p>4a. Member States shall ensure that the data protection officer has access to all data transmitted to the Passenger Information Unit and from <u>processed by the Passenger Information Unit</u> to a competent authority pursuant to Article 5. If the data protection officer considers that transmission <u>processing</u> of any data was not lawful, he or she shall <u>may</u> refer the matter to the national supervisory</p>

				<p>authority, which shall have power to order the receiving competent authority to delete that data.</p>
		<p>4b. The storage, processing and analysis of PNR data shall be carried out exclusively within a secure location within the territory of the Member States of the European Economic Area.</p>		<p>4b. The storage, processing and analysis of PNR data <u>by the PIU</u> shall be carried out exclusively within a secure location within the territory of the <i>European Union</i>.</p>
		<p>4c. Member States shall bear the costs of use, retention and exchange of PNR data.</p>	<p>Possibly acceptable if combined with recital (13a). <i>"(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</i></p>	<p>4c. Member States shall bear the costs of use, retention and exchange of PNR data. <u><i>Move to recital.</i></u></p>

			<p><i>instrument for financial support for police cooperation, preventing and combating crime, and crisis management as part of the Internal Security Fund."</i></p> <p><u>COM</u>: EP AM stating the obvious: running cost to be borne by MSs (separate from establishing a PNR system)</p> <p><u>EP</u>: Proposal to put this into recital</p>	
	<p><u>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</u></p>			<p>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</p>

	persons across borders ¹ applies, shall comply with that Code.			of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders ² applies, shall comply with that Code.
--	---	--	--	--

Article 5				
Competent authorities	Competent authorities	Competent authorities		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 take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.	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 take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.	1. Each Member State shall adopt a list of the competent authorities entitled to request or receive masked out PNR data or the result of the systematic processing of PNR data from the Passenger Information Units in order to examine that information further or take appropriate action for the specific purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime, or the prevention of an immediate and serious threat to public security . Europol shall be entitled to receive PNR data		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 take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, or the prevention of an immediate and serious threat to public security . Europol shall

¹ OJ L 105, 13.4.2006, p.1.

² OJ L 105, 13.4.2006, p.1.

		or the result of the processing of PNR data from the Passenger Information Units of the Member States within the limits of its mandate and, where necessary, for the performance of its tasks.		be entitled to request 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 authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime.	2. Competent <u>The</u> authorities <u>referred to in paragraph 1</u> shall consist of <u>be</u> competent for the prevention, detection, investigation or prosecution of terrorist offences and <u>or</u> serious crime.	2. Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious transnational crime or the prevention of immediate and serious threats to public security.		2. The authorities referred to in paragraph 1 shall be competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime [or the prevention of immediate and serious threats to public security].
3. Each Member State shall notify the list of its competent authorities to the Commission twelve months after entry into force of this Directive at the latest, and may at any time update its declaration. The Commission shall publish this information, as well as any updates, in the Official Journal of the European Union.	3. <u>For the purpose of Article 7(4),</u> Each Member State shall notify the list of its competent authorities to the Commission twelve <u>eighteen</u> months after entry into force of this Directive at the latest, and may at any time update its declaration <u>this notification</u> . The Commission shall publish this information, as well as any updates <u>modifications of it</u> , in the <i>Official Journal of the</i>	3. By ...* [12 months after the date of entry into force of this Directive], each Member State shall notify the list of its competent authorities to the Commission and shall at any time update its declaration. The Commission shall publish this information, as well as any updates, in the Official Journal of the European Union.		3. For the purpose of Article 7(4), each Member State shall notify the list of its competent authorities to the Commission twelve months after entry into force of this Directive at the latest, and shall at any time update this notification. The Commission shall publish this information, as well as any

	<i>European Union.</i>			modifications of it, in the <i>Official Journal of the European Union.</i>
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 purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.	4. The PNR data of passengers and the result of the processing of PNR data received by <u>from</u> the Passenger Information Unit may be further processed by the competent authorities of the Member States only for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.	4. The PNR data of passengers and the result of the processing of PNR data received by the Passenger Information Unit may be further processed by the competent authorities of the Member States only for the specific purpose of prevention, detection, investigation or prosecution of terrorist offences and of serious transnational crime, upon request, in accordance with Article 4(2) or for the prevention of an immediate and serious threat to public security.		4. The PNR data and the result of the processing of PNR data received by the Passenger Information Unit may be further processed by the competent authorities of the Member States only for the specific purpose of prevention, detection, investigation or prosecution of terrorist offences and of serious crime, or for the prevention of an immediate and serious threat to public security.

<p>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.</p>	<p>5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences <u>violations of criminal law</u>, or indications thereof, are detected in the course of enforcement action further to such processing.</p>	<p>5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to processing for which it was originally intended.</p>		<p>5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other violations of criminal law, or indications thereof, are detected in the course of enforcement action further to such processing for which it was originally intended.</p>
<p>6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.</p>	<p>6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.</p>	<p>6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sexual life.</p>	<p>List taken from DPD (GA), Art. 8</p>	<p>6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership and the processing of data concerning health or sexual life.</p>

Article 6

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

<p>Member States concerned.</p>	<p>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 PNR data.</u></p>	<p>and non-carrier economic operators shall transfer the PNR data to the Passenger Information Units of all the Member States concerned.</p>	<p>overs at the airports of the Member States, air carriers shall transfer the PNR data__of all passengers to the Passenger Information Units of all the Member States concerned. This also applies where an intra-EU flight has one or more stopovers at the airports of different Member States, but only in relation to Member States which are collecting PNR data.</p>
---------------------------------	--	---	---

	<p>1a. <u>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></p>		<p>Annex I ... (18) Any Advance Passenger Information (API) data collected (<u>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</u>)</p> <p>Underlined text=added GA text</p>	<p>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.</p>
<p>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 Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:</p>	<p>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 <u>referred to</u> in Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:</p>	<p>2. Air carriers and non-carrier economic operators shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:</p>		<p>2. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data</p>

<p>(a) 24 to 48 hours before the scheduled time for flight departure; and</p> <p>(b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board.</p>	<p>(a) <u>once</u> 24 to 48 hours before the scheduled time for flight departure; and</p> <p>(b) <u>once</u> immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board <u>or leave</u>.</p>	<p>(a) once, 24 to 48 hours before the scheduled time for flight departure; and</p> <p>(b) once, immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board.</p>		<p>security:</p> <p>(a) once, 24 to 48 hours before the scheduled time for flight departure; and</p> <p>(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.</p>
<p>3. Member States may 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.</p>	<p>3. Member States may <u>shall</u> 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.</p>	<p>3. Member States shall permit air carriers and non-carrier economic operators to limit the transfer referred to in point (b) of paragraph 2 to updates of the transfer referred to in point (a) of that paragraph.</p>		<p>3. Member States 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 that paragraph.</p>
<p>4. On a case-by-case basis, upon request from a Passenger Information Unit in accordance with national law, air carriers shall transfer PNR data where access earlier than that mentioned in point (a) of paragraph 2 is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime.</p>	<p>4. On a case-by-case basis <u>and where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime</u>, air carriers shall, upon request from a Passenger Information Unit in accordance with <u>the procedures provided under national law</u>, transfer PNR data where access earlier at <u>other points in time than that mentioned in point (a) of</u></p>	<p>4. On a case-by-case basis, upon request from a Passenger Information Unit in accordance with national law, air carriers and non-carrier economic operators shall transfer PNR data where access earlier than that mentioned in point (a) of paragraph 2 is necessary to assist in responding to a specific, imminent, and actual threat related to terrorist offences or serious</p>		<p>4. On a case-by-case basis <u>and where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime</u>, air carriers shall, upon request from a Passenger Information Unit in accordance with national law, , transfer PNR data at <u>other points in time than that mentioned in paragraph</u></p>

	paragraph 2 is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime (a) and (b).	transnational crime.		2, (a) and (b).
		4a. Air carriers and non-carrier economic operators shall duly inform passengers of the type of personal data being collected for law enforcement purposes, their rights regarding their data as a passenger. Such information shall be provided to passengers proactively, in an easily understandable format.	Unacceptable to MSs, places the duties/burden on companies. Partial overlap with Art. 11(5)(a). <u>COM:</u> redundant, if additional language/rights (such as "easily understandable"), incorporate in Art 11(5). <i>Tentative agreement to try to put it into Art 11(5).</i>	[deleted] <i>To be discussed.</i>

Article 7				
Exchange of information between Member States	Exchange of information between Member States	Exchange of information between Member States		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), the result of the processing of PNR data is transmitted by that Passenger Information Unit to the Passenger Information	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) , the <u>PNR data</u> or the result of the any processing thereof PNR data is transmitted by that Passenger Information Unit to the	1. Passenger Information Units shall automatically exchange data on the results of the processing of PNR data. Member States shall ensure that the results of the processing of PNR data, either analytical information obtained from PNR data or the results with regard to		1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2)(a), the PNR data or the result of any processing thereof is transmitted by that

<p>Units of other Member States where the former Passenger Information Unit 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 to their relevant competent authorities.</p>	<p>Passenger Information Units corresponding units of other Member States where the former Passenger Information Unit 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 <u>information</u> to their relevant competent authorities <u>in accordance with Article 4(4)</u>.</p>	<p>persons identified by a Passenger Information Unit in accordance with Article 4(2), which is transmitted for further examination to their relevant competent authorities in accordance with Article 4(4), is proactively transmitted by a Passenger Information Unit to the Passenger Information Units of the other Member States without delay. The Passenger Information Unit of the receiving Member States shall transmit such results of the processing of PNR data to their relevant competent authorities, in accordance with Article 4(4). Where appropriate, an alert shall be entered in accordance with Article 36 of Council Decision 2007/533/JHA³.</p>		<p>Passenger Information Unit to the corresponding units of <i>all</i> other Member States where 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 the received information to their competent authorities in accordance with Article 4(4).</p>
--	--	---	--	--

³ Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

<p>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 Article 9(1), and, if necessary, also the result of the processing of PNR data. The 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).</p>	<p>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 <u>and have not yet been depersonalised through masking out under Article 9(42)</u>, and, if necessary, also the result of the <u>any</u> processing of PNR data thereof, if it has already <u>been prepared pursuant to Article 4(2)(a)</u>. The <u>duly reasoned</u> 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). <u>In case the requested data</u></p>	<p>2. Passenger Information Units shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(1) and, if necessary, also the result of processing thereof, if it has already been prepared pursuant to points (a) and (b) of Article 4(2). The duly reasoned request for such data shall be strictly limited to the data necessary in the specific case and may be based on any one or a combination of data elements, as deemed necessary by the requesting Passenger Information Unit for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious transnational crime or for the prevention of an immediate and serious threat to public security. Passenger Information Units shall provide the requested data as soon as possible using the common protocols and supported data formats. Such a request shall be justified in writing.</p>		<p>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 and have not yet been depersonalised through masking out under Article 9(2), and, if necessary, also the result of any processing 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</p>
---	---	--	--	--

	<p><u>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).</u></p>			<p>practicable. 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).</p>
<p>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</p>	<p>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</p>	<p>3. Passenger Information Units shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that have been already masked out and 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 the most</p>		

<p>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.</p>	<p>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.</p>	<p>exceptional circumstances in response to a specific real-time threat or with regard to a specific investigation or prosecution related to terrorist offences or serious transnational crime <i>or to the prevention of an immediate and serious threat to public security</i>. Such access to the full PNR data shall be permitted only with the approval of the Head of the requested Passenger Information Unit.</p>		
<p>4. Only 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). 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</p>	<p>4. <u>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</u> 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 <u>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</u></p>	<p>4. Only 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). 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</p>		<p>3. Only when necessary in cases of emergency and under the conditions laid down in paragraph 2 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. The requests from the competent authorities, a copy of which shall always be sent to the Passenger Information Unit of the requesting Member State, shall be</p>

<p>matter of priority. In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.</p>	<p>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.</p>	<p>other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.</p>		<p>reasoned. In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.</p>
<p>5. Exceptionally, where early access 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 have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights landing in or departing from the latter's territory at any time.</p>	<p>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.</p>	<p>5. Exceptionally, where early access is strictly necessary to respond to a specific and actual threat related to terrorist offences or serious transnational crime or to prevent an immediate and serious threat to public security, the Passenger Information Unit of a Member State shall have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights landing in or departing from the latter's territory at any time, where such data has been retained. That procedure shall cover only requests for the PNR data already collected and</p>		<p>5. Exceptionally, where access to PNR data is necessary to respond to a specific and actual threat related to terrorist offences or serious crime [or to prevent an immediate and serious threat to public security], 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 obtain PNR data in accordance with article 6(4) and provide it to the requesting Passenger Information Unit. [That procedure shall cover</p>

		retained by the Passenger Information Unit which is requested to provide the data.		only requests for the PNR data already collected and retained by the Passenger Information Unit which is requested to provide the data.]
6. Exchange of information under this Article may take place using any existing channels for international law enforcement cooperation. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contacts to which requests may be sent in cases of urgency. The Commission shall communicate to the Member States the notifications received.	6. Exchange of information under this Article may take place using any existing channels for international law enforcement cooperation <u>between the competent authorities of the Member States</u> . The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contacts <u>points</u> to which requests may be sent in cases of urgency <u>emergency</u> . The Commission shall communicate to the Member States the notifications received.	6. Exchange of information under this Article shall take place using existing channels for Union and international law enforcement cooperation, in particular Europol, its 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 contacts to which requests may be sent in cases of urgency. The Commission shall communicate to the Member States the notifications received.		6. Exchange of information under this Article may take place using any existing channels for cooperation between the competent authorities of the Member States. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contact points to which requests may be sent in cases of emergency. The Commission shall communicate to the Member States the notifications received.
		6a. Where analytical		

		information obtained from PNR is transferred pursuant to this Directive, the safeguards provided for in paragraph 1 shall be complied with.		
Article 7a:				
		Conditions for access to PNR data by Europol		Conditions for access to PNR data by Europol
		1. Europol may submit, on a case-by-case basis, an electronic and duly reasoned request to the Passenger Information Unit of any Member State for the transmission of specific PNR data or the results of the processing of specific PNR data, when this is strictly necessary to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious transnational 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	(20a) The exchange of information through a secure Union system for the exchange of PNR data between Member States and between Member States and Europol should be guaranteed. The development and operational management of that system could be the responsibility of Europol. A one-stop shop could be created as part of that system to register and transmit the requests for information exchanges. The European Data Protection Supervisor should be responsible for monitoring the processing of the personal data performed through this Union system for exchange of PNR data	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 a crime is within Europol's competence pursuant to Decision 2009/371/JHA. The reasoned request shall set

		<p>the results of the processing of PNR data will substantially contribute to the prevention, detection, investigation or prosecution of the criminal offence concerned.</p>	<p>with Europol.</p>	<p>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.</p>
		<p>2. Upon receipt of a request by Europol, a court or an independent administrative body of the Member State shall verify, in a timely manner, whether all the conditions set out in paragraph 1 are met. The Passenger Information Unit shall provide the requested data to Europol as soon as practicable, provided that those conditions are met.</p>		<p>[deleted]</p>
		<p>3. Europol shall inform the data protection officer appointed in accordance with Article 28 of Decision 2009/371/JHA of each exchange of information under this Article.</p>		<p>3. Europol shall inform the data protection officer appointed in accordance with Article 28 of Decision 2009/371/JHA of each exchange of information</p>

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

Article 8				
Transfer of data to third countries	Transfer of data to third countries States	Transfer of data to third countries		Transfer of data to third States
A Member State may transfer PNR data and the results of the processing of PNR data to a third country, only on a case-by-case basis and if:	A Member State may transfer PNR data and as well <u>as</u> the results of the processing of PNR <u>such</u> data <u>stored by the Passenger Information Unit in accordance with Article 9</u> to a third country,	1. A Member State may transfer PNR data and the results of the processing of PNR data to a third country, only on a case-by-case basis, subject to a duly reasoned request based on sufficient	Align to DPD Art. 34 Ad end of para: "transfers on a systematic basis": no, risky, only case-by-case	A Member State may transfer PNR data as well as the results of the processing of such data stored by the Passenger Information Unit in accordance with Article 9

<p>(a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled,</p> <p>(b) the transfer is necessary for the purposes of this Directive specified in Article 1(2), and</p> <p>(c) the third country agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive specified in Article 1(2) and only with the express authorisation of the Member State.</p>	<p>only on a case-by-case basis and if:</p> <p>(a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled,</p> <p>(b) the transfer is necessary for the purposes of this Directive specified in Article 1(2), and</p> <p>(c) the third country agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive specified in Article 1(2) and only with the express authorisation of the Member State.</p> <p><u>(d) similar conditions as those laid down in Article 7(2) are fulfilled.</u></p>	<p>evidence, where the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences, the prevention of an immediate and serious threat to public security or the execution of criminal penalties and the receiving competent authority in the third country is responsible for the prevention, investigation, detection or prosecution of criminal offences, the prevention of an immediate and serious threat to public security or the execution of criminal penalties, provided that:</p> <p>(a) the third country concerned ensures an adequate level of protection as referred to in Directive 95/46/EC of the European Parliament and of the Council⁴ for the intended data processing, subject to meeting all the other conditions laid down in this Directive;</p>		<p>to a third country, only on a case-by-case basis and if</p> <p>(a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled,</p> <p>(b) the transfer is necessary for the purposes of this Directive specified in Article 1(2), and</p> <p>(c) the third country agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive specified in Article 1(2) and only with the express authorisation of the Member State.</p> <p>(d) similar <i>adequate</i></p>
---	--	---	--	---

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

		<p>(b) the Member State from which the data were obtained has given its consent to the transfer in compliance with national law.</p> <p>In exceptional circumstances, transfers of PNR data without prior consent in accordance with paragraph 1 shall be permitted only if such transfers are essential for the prevention of an immediate and serious threat to public security of a Member State or a third country or to protect the essential interests of a Member State and prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay and the transfer shall be duly recorded and subject to an ex-post verification.</p> <p>By way of derogation from the first subparagraph, transfers of data shall be permitted on a systematic basis following the</p>		<p>conditions as those laid down in Article 7(2) are fulfilled.</p> <p>In exceptional circumstances, transfers of PNR data without prior consent shall be permitted only if such transfers are essential for the prevention of an immediate and serious threat to public security of a Member State or a third country or to protect the essential interests of a Member State and prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay and the transfer shall be duly recorded and subject to an ex-post verification.</p>
--	--	--	--	--

		conclusion of an international agreement between a third country and the Union.		
		2. Member States shall transfer PNR data to competent authorities of third countries only under terms consistent with this Directive and only upon ascertaining that the use that the recipients intend to make of the PNR is consistent with those terms and safeguards.		2. Member States shall transfer PNR data to competent authorities of third countries only under terms consistent with this Directive and only upon ascertaining that the use that the recipients intend to make of the PNR is consistent with those terms and safeguards.
		3. Onward transfers to other third countries shall be prohibited.		3. <i>Onward transfers from one third country to another shall be prohibited.</i>
		4. Where PNR data relating to a citizen or a resident of another Member State are transferred to a third country, the competent authorities of that Member State shall be informed of the matter at the earliest appropriate opportunity.		
		5. The data protection officer shall be informed each time a Member State transfers PNR data pursuant to this Article. The data protection officer shall inform the]	5. The data protection officer shall be informed each time a Member State transfers PNR data pursuant to this Article.

		national supervisory authority of the transmission of data pursuant to this Article on a regular basis.		
--	--	--	--	--

DRAFT 16 NOV		Article 9		
Period of data retention	Period of data retention	Period of data retention		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 after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.	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 <u>five years</u> after their transfer <u>transmission</u> to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.	1. Member States shall ensure that the PNR data provided by the air carriers and non-carrier economic operators to the Passenger Information Unit pursuant to Article 4(2) are retained in a database at the Passenger Information Unit for a period of 30 days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.		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 5 years after their <u>transmission</u> to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.
2. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall	2. Upon expiry of the period of 30 days <u>two years</u> after the transfer of the PNR data to the Passenger Information Unit <u>as referred to in paragraph 1, the PNR data shall be retained at</u>	2. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be retained at		2. Upon expiry of the period of 30 days <u>6 months</u> after the transfer of the PNR data to the Passenger Information Unit <u>as referred to in paragraph 1, the PNR</u>

<p>be retained at the Passenger Information Unit for a further period of five years. During this period, all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such 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.</p> <p>For the purposes of this Directive, the data elements which could serve</p>	<p>the Passenger Information Unit for a further period of five years. During this period, all <u>depersonalised through masking out of the following</u> data elements which could serve to <u>directly</u> identify the passenger to whom <u>the</u> 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)(e) 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.</p> <p>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</p>	<p>the Passenger Information Unit for a further period of five years. During this period, all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such masked out PNR data shall be accessible only to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria according to point (d) of Article 4(2).</p> <p>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:</p> <ul style="list-style-type: none"> – Name(s), including the names of other passengers on PNR and number of travellers on PNR travelling together; – Address and contact 		<p>data shall be <i>retained at the Passenger Information Unit for a further period of five years. During this period all PNR data shall be <u>depersonalised through masking out of the following</u> data elements which could serve to <u>directly</u> identify the passenger to whom <u>the</u> 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)(e) 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.</i></p> <p>For the purposes of this Directive, the data elements which could serve to identify</p>
--	--	--	--	---

<p>to identify the passenger to whom PNR data relate and which should be filtered and masked out are:</p> <ul style="list-style-type: none"> - Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together; - Address and contact information; - General remarks to the extent that it contains any information which could serve to identify the passenger to whom PNR relate; and - Any collected Advance Passenger Information. 	<p>out are:</p> <ol style="list-style-type: none"> <u>1. Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together;</u> <u>2. Address and contact information;</u> <u>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;</u> <u>4. Frequent flyer information;</u> 5. General remarks to the extent that it contains any information which could serve to <u>directly</u> identify the passenger to whom <u>the</u> PNR relate; and <u>6. Any collected Aadvance Ppassenger information.</u> 	<p>information;</p> <ul style="list-style-type: none"> - General remarks to the extent that it contains any information which could serve to identify the passenger to whom PNR relate; and - Any collected Advance Passenger Information. 		<p>the passenger to whom PNR data relate and which should be filtered and masked out are:</p> <ol style="list-style-type: none"> <u>1. Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together;</u> <u>2. Address and contact information;</u> <u>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;</u> <u>4. Frequent flyer information;</u> 5. General remarks to the extent that it contains any information which could serve to <u>directly</u> identify the passenger to whom <u>the</u> PNR relate; and <u>6. Any collected Aadvance Ppassenger information.</u>
		<p>2a. After consulting the data protection officer for the purposes of point (b) of</p>	<p>GA, Art. 7(2), last part <u>In case the requested data</u></p>	

		<p>Article 4(2), the national supervisory authority shall authorise re-identification of masked out PNR data and access to the full PNR data where it reasonably believes that such re-identification is necessary to carry out an investigation in response to a specific and actual threat or risk relating to terrorist offences, to carry out a specific investigation or prosecution relating to a serious transnational crime, or to prevent an immediate and serious threat to public security. Such access to the full data shall be allowed for a period of four years after the data has been masked out in cases concerning serious transnational crime and for the entire five-year period referred to in paragraph 2 in</p>	<p><u>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).</u></p> <p>EP suggested AM for a new para 2a has been merged with para 3.</p>	
	<p><u>3. Upon expiry of the two-year 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)</u></p>			<p><u>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</u></p>

	<p><u>and 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.</u></p>			<p><i>Article 4(2)(b). <u>Disclosure of the full PNR data can be permitted only when approved by a judicial authority or, following consultation of the data protection officer of the Passenger Information Unit, by another national authority competent under national law to verify whether the conditions for disclosure are fulfilled.</u></i></p>
<p>3. Member States shall ensure that the PNR data are deleted upon expiry of the period specified in paragraph 2. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.</p>	<p>34. Member States shall ensure that the PNR data are deleted upon expiry of the period specified in paragraph 2 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations case for the purpose of prevention, detection, investigation or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.</p>	<p>3. Member States shall ensure that the PNR data are deleted permanently upon expiry of the period specified in paragraph 2. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.</p>		<p>34. 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 prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.</p>

<p>4. The result of matching referred to in Article 4(2)(a) and (b) shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities of a positive match. Where the result of an automated matching operation has, further to individual review by non-automated means, proven to be negative, it shall, however, be stored so as to avoid future ‘false’ positive matches for a maximum period of three years unless the underlying data have not yet been deleted in accordance with paragraph 3 at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.</p>	<p>45. The result of matching<u>the processing</u> referred to in Article 4(2)(a) and (b) shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities of a positive match. Where the result of an automated matching operation<u>processing</u> has, further to individual review by non-automated means <u>as referred to in Article 4(2)(a) last subparagraph</u>, proven to be negative, it shall<u>may</u>, however, be stored so as to avoid future ‘false’ positive matches for a maximum period of three years unless<u>as long as</u> the underlying data have not yet been deleted in accordance with paragraph 3<u>1</u> at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.</p>	<p>4. The result of matching referred to in points (a) and (b) of Article 4(2) shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities of a positive match. Where the result of an automated matching operation has, subject to human intervention by a member of the Passenger Information Unit, proven to be negative, it shall, however, be stored so as to avoid future ‘false’ positive matches for a maximum period of three years unless the underlying data have not yet been deleted in accordance with paragraph 3 at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.</p>		<p>45. The result of matching<u>the</u> 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<u>processing</u> has, further to individual review by non-automated means <u>as referred to in Article 4(2)(a) last subparagraph</u>, proven to be negative, it shall<u>may</u>, however, be stored so as to avoid future ‘false’ positive matches for a maximum period of three years unless<u>as long as</u> the underlying data have not yet been deleted in accordance with paragraph 3<u>1</u> at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.</p>
---	--	--	--	---

Article 10

**Penalties against air carriers
and non-carrier economic
operators**

1a. All data held by air carriers and non-carrier economic operators shall be held in a secure database on a security accredited computer system, that either meets or exceeds international industrial standards.

~~1a. All data held by air carriers and non carrier economic operators shall be held in a secure database on a security accredited computer system, that either meets or exceeds international industrial standards.~~

Article 11

Protection of personal data	Protection of personal data	Protection of personal data		
<p>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 access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as those adopted under national law in implementation of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA. The provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable.</p>	<p>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 access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as those adopted under national law in <u>implementation of</u> Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA. The provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable.</p>	<p>1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as laid out in national and Union law, and in the implementation of Articles 17, 18, 19 and 20 of the Framework Decision 2008/977/JHA. Those Articles shall therefore be applicable.</p>		
<p>2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of the Council Framework Decision 2008/977/JHA regarding</p>	<p>2. Each Member State shall provide that the provisions adopted under <u>the</u> national law in <u>to</u> implementation of Articles 21 and 22 of the Council Framework Decision 2008/977/JHA regarding confidentiality of</p>	<p>2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of the Framework Decision 2008/977/JHA regarding confidentiality of processing and data security</p>		

<p>confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.</p>	<p>processing and data security shall also apply to all processing of personal data pursuant to this Directive</p>	<p>shall also apply to all processing of personal data pursuant to this Directive.</p>		
		<p>2a. Where provisions adopted under national law in implementation of Directive 95/46/EC provide the passenger with greater rights related to the processing of their data than with this Directive, those provisions shall apply.</p>		
<p>3. Any processing of PNR data revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life shall be prohibited. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately.</p>	<p>3. Any processing of PNR data revealing a person's race <u>racial</u> or ethnic origin, <u>political opinions</u>, religious or philosophical belief, political opinion, trade union membership, health or sexual life shall be prohibited. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted <u>immediately without delay</u>.</p>	<p>3. Member States shall prohibit the processing of PNR data from revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sexual life. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately.</p>	<p>Agreed at the 2nd trilogue to take the list from the Data Protection Directive in order not to have more diverging lists.</p>	<p>3. Member States shall prohibit the processing of PNR data from revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership or activities, and the processing of data concerning health or sexual life. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be</p>

				deleted immediately
--	--	--	--	----------------------------

		<p>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:</p> <p>(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;</p> <p>(b) the requests by competent authorities and Passenger Information Units of other Member States and the recipients of the processed PNR data;</p> <p>(c) all requests and transfers of data to a third country, the identification of that third country and the legal grounds on which the data are transferred;</p> <p>(d) the time limits for retention and erasure of</p>	<p>Concerning 3a(a) and persons to have access: In particular worries from smaller MSs that a too strict limitation will pose difficulties/be operationally unmanageable and maybe even counterproductive.</p>	<p>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:</p> <p>(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;</p> <p>(b) the requests by competent authorities and Passenger Information Units of other Member States and the recipients of the processed PNR data;</p> <p>(c) all requests and transfers of data to a third country, the identification of that third country and the</p>
--	--	---	--	--

		<p>different categories of data.</p> <p>The Passenger Information Unit shall make all documentation available, on request, to the national supervisory authority.</p>		<p>legal grounds on which the data are transferred;</p> <p>(d) the time limits for retention and erasure of different categories of data.</p> <p>The Passenger Information Unit shall make all documentation available, on request, to the national supervisory authority.</p>
--	--	---	--	---

		<p>3b. Member States shall ensure that the Passenger Information Unit keeps records of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed 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.</p>		<p>3b. Member States shall ensure that the Passenger Information Unit keeps records of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The records of consultation and disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed 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</p>
--	--	---	--	--

		<p>The persons who operate security controls, access and analyse the PNR data, and operate the data logs, shall be security cleared and security trained. They shall have a profile which establishes and limits the records which they are authorised to access in accordance with the nature of their work, role, and legal entitlement.</p> <p>The records shall be kept for a period of four years. However, where in accordance with Article 9(3), the underlying data have not been deleted at the end of that four-year period, the records shall be kept until the underlying data are deleted.</p>		
--	--	---	--	--

		<p>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.</p>		<p>The persons who operate security controls, access and analyse the PNR data, and operate the data logs, shall be security cleared and security trained. They shall have a profile which establishes and limits the records which they are authorised to access in accordance with the nature of their work, role, and legal entitlement.</p> <p>The records shall be kept for a period of four <u>five</u> years. However, where in accordance with Article 9(3), the underlying data have not been deleted at the end of that four-year period, the records shall be kept until the underlying data are deleted.</p> <p>3c. Member States shall ensure that their Passenger Information Unit implements</p>
--	--	---	--	--

				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.
--	--	--	--	---

		<p>3d. Member States shall ensure that where a personal data breach is likely to affect 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.</p>		<p>3d. Member States shall ensure that where a personal data breach is likely to affect <u>result in a high risk</u> 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.</p>
<p>4. All processing of PNR data by air carriers, all transfers of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States and third countries, even if refused, shall be logged or documented by the Passenger Information Unit and the competent authorities for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of data processing, in particular by</p>	<p>4. All processing, <u>including receipt</u> of PNR data by <u>from</u> air carriers, all transfers of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States and third countries, even if refused, shall be logged or documented by the Passenger Information Unit and the competent authorities for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data</p>	<p>4. All processing of PNR data by air carriers, all transfers of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States and third countries, even if refused, shall be logged or documented by the Passenger Information Unit and the competent authorities for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of data processing, in particular by the national data</p>		

<p>the national data protection supervisory authorities. These logs shall be kept for a period of five years unless the underlying data have not yet been deleted in accordance with Article 9(3) at the expiry of those five years, in which case the logs shall be kept until the underlying data are deleted.</p>	<p>integrity and security of data processing, in particular by the national data protection supervisory authorities. These logs shall be kept for a period of five years unless the underlying data have not yet been deleted in accordance with Article 9(34) at the expiry of those five years, in which case the logs shall be kept until the underlying data are deleted.</p>	<p>protection — supervisory authorities. These logs shall be kept for a period of five years unless the underlying data have not yet been deleted in accordance with Article 9(3) at the expiry of those five years, in which case the logs shall be kept until the underlying data are deleted.</p>		
<p>5. Member States shall ensure that air carriers, their agents or other ticket sellers for the carriage of passengers on air service inform passengers of international flights at the time of booking a flight and at the time of purchase of a ticket in a clear and precise manner about the provision of PNR data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and serious crime, the possibility of exchanging and sharing such data and their data protection rights, in particular the right to</p>	<p>5. Member States shall ensure that air carriers, their agents or other ticket sellers for the carriage of passengers on air service inform passengers of international flights at the time of booking a flight and at the time of purchase of a ticket in a clear and precise manner about the provision of PNR <u>transmission</u> data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and serious crime, the possibility of exchanging and sharing such data and their data protection rights, in</p>	<p>5. Member States shall ensure that air carriers and non-carrier economic operators inform passengers of international flights at the time of booking a flight and at the time of purchase of a ticket in a clear and precise manner about the provision of PNR data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and serious transnational crime, the possibility of exchanging and sharing such data and their data protection rights, such as the right to access, correction, erasure and</p>		

<p>complain to a national data protection supervisory authority of their choice. The same information shall be made available by the Member States to the public.</p>	<p>particular the right to complain to a <u>the competent</u> national data protection supervisory authority of their choice. The same information shall be made available by the Member States to the public.</p>	<p>blocking of data, and in particular the right to lodge a complaint to a national supervisory authority of their choice.</p>		
		<p>5a. Member States shall also ensure that their Passenger Information Unit provides the data subject with the information with regard to the rights referred to in paragraph 5 and how to exercise those rights.</p>		<p><i>Member States shall ensure that individuals are provided with information relating to their rights and how to exercise those rights.</i></p>
<p>6. Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited.</p>	<p>6. Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited.</p>	<p>6. Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited.</p>		
<p>7. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant</p>	<p>7. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to</p>	<p>7. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of <i>all</i> the provisions of this Directive and shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Directive. National</p>		<p>7. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of <i>all</i> the provisions of this Directive and shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of</p>

to this Directive.	this Directive.	supervisory authorities shall take disciplinary action against persons responsible for any intentional breach of privacy, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.		infringements of the provisions adopted pursuant to this Directive. <i>National supervisory authorities shall take disciplinary action against persons responsible for any intentional breach of privacy, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.</i>
		7a. Any transfer of PNR data by competent authorities or Passenger Information Units to private parties in Member States or in third countries shall be prohibited. Any wrongful conduct shall be penalised.		<i>7a. Any transfer of PNR data by competent authorities or Passenger Information Units to private parties in Member States or in third countries shall be prohibited. Any wrongful conduct shall be penalised.</i>
Article 12				
National supervisory authority	National supervisory authority	National supervisory authority		
Each Member State shall provide that the national supervisory authority established in implementation of Article 25	Each Member State shall provide that the national supervisory authority <u>or authorities established in to</u> implementation of Article 25	Each Member State shall provide that the national supervisory authority established in implementation of Article 25 of Framework		Each Member State shall provide that the national supervisory authority established in to implementation of

<p>of Framework Decision 2008/977/JHA shall also be responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to the present Directive. The further provisions of Article 25 Framework Decision 2008/977/JHA shall be applicable.</p>	<p>of Framework Decision 2008/977/JHA shall also be responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to the present Directive. The further provisions of Article 25 Framework Decision 2008/977/JHA shall be applicable.</p>	<p>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.</p>		<p>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.</p>
		<p>Article 12a</p>		
		<p>Duties and powers of the national supervisory authority</p>		
		<p>1. The national supervisory authority of each Member State shall be responsible for monitoring the application of the provisions adopted pursuant to this Directive and for contributing to its consistent application throughout the Union, in order to protect fundamental rights in relation to the processing of personal data. Each national supervisory authority shall:</p> <p>(a) hear complaints lodged</p>		<p><i>1. The national supervisory authority of each Member State shall be responsible for monitoring the application of the provisions adopted pursuant to this Directive—and for contributing to its consistent application throughout the Union, in order with a view to protect fundamental rights in relation to the processing of personal</i></p>

		<p>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, in particular where further investigation or coordination with another national supervisory authority is necessary, such complaints having been brought by any individual, regardless of nationality, country of origin, or place of residence;</p> <p>(b) exercise effective powers of oversight, investigation, intervention and review, and have the power to refer infringements of law related to this Directive for prosecution or disciplinary action, where appropriate;</p> <p>(c) check the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint, and inform the data subject concerned, if the data</p>	<p><i>data. Each national supervisory authority shall:</i></p> <p><i>(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; in particular where further investigation or coordination with another national supervisory authority is necessary, such complaints having been brought by any individual, regardless of nationality, country of origin, or place of residence;</i></p> <p><i>(b) exercise effective powers of oversight, investigation, intervention and review, and have the power to refer infringements of law related to this Directive for prosecution or disciplinary action, where appropriate;</i></p>
--	--	--	---

		<p>subject has addressed a complaint, of the outcome of the investigations within a reasonable time period;</p> <p>(d) monitor relevant developments, insofar as they have an impact on the protection of person data, in particular the development of information and communication technologies.</p> <p>Member States shall provide a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat.</p>	<p><i>(c) check the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint, and inform the data subject concerned, if the data subject has addressed a complaint, of the outcome of the investigations within a reasonable time period;</i></p> <p><i>(d) monitor relevant developments, insofar as they have an impact on the protection of person data, in particular the development of information and communication technologies.</i></p> <p><i>Member States shall provide a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat.</i></p>
--	--	---	--

		<p>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 and, where appropriate, cooperate with national supervisory authorities of other Member States to that end.</p>		<p><i>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— and, —where appropriate, —cooperate with —national supervisory —authorities of other Member States to that end.</i></p>
		<p>3. For complaints referred to in point (a) of paragraph 1 the national supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.</p>		<p><i>3. —For —complaints referred to in point (a) of paragraph 1 the national supervisory —authority shall —provide —a complaint —submission form, —which —can —be completed electronically, without excluding other means —of communication.</i></p>

		<p>4. Member States shall ensure that the performance of the duties of their national supervisory authority is free of charge for the data subject. However, where requests are manifestly excessive, in particular due to their repetitive character, the national supervisory authority may charge a reasonable fee.</p>		<p><i>4. Member States shall ensure that the performance of the duties of their national supervisory authority is free of charge for the data subject. However, where requests are manifestly excessive, in particular due to their repetitive character, the national supervisory authority may charge a reasonable fee.</i></p>
		<p>5. Each Member State shall ensure that their national supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers.</p>		<p><i>5. Each Member State shall ensure that their national supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers.</i></p>
		<p>6. Each Member States shall ensure that their national supervisory authority has its own staff which are appointed by, and subject to, the direction of the Head of the national supervisory authority.</p>		<p><i>6. Each Member States shall ensure that their national supervisory authority has its own staff which are appointed by, and subject to, the direction of the Head of the</i></p>

				<i>national</i> — <i>supervisory</i> <i>authority.</i>
--	--	--	--	---

		7. In the performance of their duties, members of the national supervisory authority shall neither seek nor take instruction from anybody, and shall maintain complete independence and impartiality.	7. In the performance of their duties, members of the national supervisory authority shall neither seek nor take instruction from anybody, and shall maintain complete independence and impartiality.
--	--	---	--

Article 13

Common protocols and supported data formats	Common protocols and supported data formats	Common protocols and supported data formats		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, in the event of technical failure, 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.	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, in the event of technical failure, 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.	1. All transfers of PNR data, by air carriers and by non-carrier economic operators , to the Passenger Information Units for the purposes of this Directive shall be made by electronic means which provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. In the event of technical failure, the PNR		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 which provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. In the event of

		<p>data shall be transferred by any other appropriate means whilst maintaining the same level of security and in full compliance with Union data protection law.</p>		<p>technical failure, the PNR data shall be transferred by any other appropriate means whilst maintaining the same level of security and in full compliance with Union data protection law.</p>
<p>2. Once the period of one year from the date of adoption of the common protocols and supported data formats has elapsed, all transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.</p>	<p>2. Once the period of one year from the date of adoption, <u>for the first time</u>, of the common protocols and supported data formats <u>by the Commission in accordance with paragraph 3</u>, 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 <u>those</u> 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</p>	<p>2. Once the period of one year from the date of adoption of the common protocols and supported data formats has elapsed, all transfers of PNR data by air carriers and by non-carrier economic operators to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.</p>		<p>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</p>

	for their transfers.			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 procedure referred to in Article 14(2).	3. The list of accepted common protocols and supported data formats shall be drawn up <u>taking due account of ICAO regulations</u> and, if need be, adjusted, by the Commission <u>by means of implementing acts</u> in accordance with the procedure referred to in Article 14(2).	3. The Commission shall be empowered to adopt delegated acts in accordance with Article 14 concerning the adoption and, if necessary, adjustment of a list of accepted common protocols and supported data formats.	This concerns the uniform conditions for the implementation of the Directive, therefore implementing acts (Article 291 TFEU) is the appropriate type of acts. The essential elements and the conditions for the exercise of the implementing power are set out in Article 13(1).	3. The list of accepted common protocols and supported data formats shall be drawn up and, if necessary, adjusted by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 14(2). <i>Delegated / Implementing Acts to be discussed.</i>

<p>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.</p>	<p>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.</p>	<p>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.</p>		<p>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.</p>
<p>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.</p>	<p>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 <u>paragraph 2.</u></p>	<p>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.</p>		<p>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—referred to in paragraph 2.</p>

Article 14

Committee procedure	Committee procedure	<u>Delegated Acts</u>		Committee procedure
<p>1. The Commission shall be assisted by a committee ('the Committee'). That Committee shall be a committee within the meaning of Regulation [.../2011/EU] of 16 February 2011.</p>	<p>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.</p>	<p>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</p>	<p>The list of accepted common protocols and supported data formats concerns the uniform conditions for the implementation of the Directive, therefore implementing acts (Article 291 TFEU) is the appropriate type of acts.</p>	

<p>2. Where reference is made to this paragraph, Article 4 of Regulation [.../2011/EU] of 16 February 2011 shall apply.</p>	<p>2. Where reference is made to this paragraph, Article 4⁵ of Regulation [.../2011/EU] of 16 February No. 182/2011 shall apply.</p>	<p>2. The power to adopt delegated acts referred to in Article 13(3) shall be conferred on the Commission for a period of [X] years from ...* [the date of entry into force of this Directive]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the [X] year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.</p>		
		<p>2a. The delegation of power referred to in Article 13(3) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date</p>		

		specified therein. It shall not affect the validity of any delegated acts already in force.		
		2b. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.		
		2c. A delegated act adopted pursuant to Article 13(3) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.		

		<p>3. The delegation of power referred to in Article 14 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</p>		
		<p>4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</p>		
		<p>5. A delegated act adopted pursuant to Article 14 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of [two months] of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European</p>		

Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.

**CHAPTER V
FINAL PROVISIONS**

Article 15

Transposition	Transposition	Transposition		Transposition
<p>1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest two years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.</p> <p>When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the</p>	<p>1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest two years 36 months after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.</p> <p>When Member States adopt those provisions, they shall contain a reference to this Directive or be</p>	<p>1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest two years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.</p> <p>When Member States adopt those provisions, they shall contain a reference to this Directive or be</p>	<p>Consistent with practice regarding Directives; horizontal position of the Council.</p>	<p>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.</p> <p>When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a</p>

occasion of their official publication. Member States shall determine how such reference is to be made.	accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.	accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.		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.	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.	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.		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	Transitional provisions	Transitional provisions		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	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.	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.		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

to in Article 6(1) are collected.				referred to in Article 15, the PNR data from all flights referred to in Article 6(1) are collected.
Article 17				
Review	Review	Review		Review
	1. <u>The Council shall, at the appropriate level, discuss regularly the practical experiences and relevant issues within the scope and subject matter of the Directive.</u>			1. The Council shall, at the appropriate level, discuss regularly the practical experiences and relevant issues within the scope and subject matter of the Directive.
<p>On the basis of information provided by the Member States, the Commission shall:</p> <p>(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. The Commission shall submit a report to the European Parliament and the Council within two years after the date mentioned in Article</p>	<p>2. On the basis of <u>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 undertake a review of the operation of this Directive and:</u></p> <p>(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. The Commission shall submit a</p>	<p>On the basis of information provided by the Member States, the Commission shall, by ...*[four 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 <i>to</i> the Council. That review shall cover all the elements of this Directive.</p> <p>In conducting its review, the Commission shall pay special attention to compliance with the</p>		<p>2. 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, by ...*[three years after the date of transposition referred to in Article 15(1)], conduct a review of the operation of this all the elements of this Directive and submit and present an evaluation, to the</p>

<p>15(1);</p> <p>(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, the length of the data retention period and the quality of the assessments. It shall also contain the statistical information gathered pursuant to Article 18.</p>	<p>report to the European Parliament and the Council within two years after the date mentioned in Article 15(1);</p> <p>(b) — undertake a review of the operation of this Directive and submit a report to the European Parliament and the Council <u>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.</u></p> <p>(b) within four years after the date mentioned in Article 15(1). Such review shall cover all the submit a report to the European Parliament and the Council <u>on all other elements of this Directive and on the feasibility and necessity of including transportation providers other than air carriers in the scope of this Directive, taking into account the experience gained by Member States, especially</u></p>	<p>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. It shall also contain the statistical information gathered pursuant to Article 18;</p> <p>After consulting the relevant Union agencies, the Commission shall, by ...* [two years after the date of transposition of this Directive referred to in Article 15(1)], submit an initial evaluation report to the European Parliament and to the Council.</p>		<p>European Parliament and to the Council.</p> <p>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, as well as its compliance with the European Court of Justice ruling on the Data Retention Directive, including the length of the data retention period and the quality of the assessments and the effectiveness of the sharing of data between the Member States, and the quality of the assessment including with regard to the statistical information gathered pursuant to Article 18. It shall also contain the statistical information gathered</p>
--	---	--	--	---

	<p>those Member States that <u>collect PNR from other transportation providers</u> with special attention to the compliance with standard of protection of personal data, the length of the data retention period and the quality of the assessments. It shall also contain the statistical information gathered pursuant to Article 18.</p>			<p>pursuant to Article 18.</p> <p>The report submitted shall also include a review on the feasibility and necessity, <i>proportionality, and effectiveness of the collection and transfer</i> of including all or selected intra-EU flights in the scope of this Directive, <i>including the possibility of the collection of intra-EU flights</i> 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.</p> <p>[After consulting the relevant Union agencies, the Commission shall, by ...* [four years after the entry into force of this Directive], submit an initial evaluation report to the European Parliament and to the</p>
--	---	--	--	--

				Council].
	<p><u>3. 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.</u></p>			<p>3. 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.</p>

Article 18

Statistical data	Statistical data	Statistical data		
<p>1. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units. Such statistics shall as a minimum cover the number of identifications of any persons who may be involved in a terrorist offence or serious crime according to Article 4(2) and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination.</p>	<p>1. Member States shall prepare <u>provide on a yearly basis the Commission with</u> a set of statistical information on PNR data provided to the Passenger Information Units. Such <u>These statistics shall not contain any personal data.</u></p>	<p>1. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units. Such statistics shall as a minimum cover the number of identifications of any persons who may be involved in a terrorist offence or transnational serious crime according to Article 4(2) and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination, including the number of investigation and convictions that have resulted from the collection of PNR data in each Member State.</p>	<p>Redundant in view of paragraph 2</p>	<p>1. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units. These statistics shall not contain any personal data.</p>
<p>2. These statistics shall not contain any personal data. They shall be transmitted to the Commission on a yearly basis.</p>	<p>2. <u>The</u> statistics shall as a minimum cover the (a) <u>total</u> number of identifications of any persons who may be involved in a terrorist offence or serious crime according to Article 4(2) <u>passengers whose PNR data were collected and</u></p>	<p>2. These statistics shall not contain any personal data. They shall be transmitted to the European Parliament, the Council and the Commission every two years.</p>		<p>2. The statistics shall as a minimum cover (a) total number of passengers whose PNR data were collected and exchanged; (b) number of passengers identified for further scrutiny;</p>

	<p><u>exchanged;</u></p> <p>(b) <u>number of passengers identified for further scrutiny;</u></p> <p>(c) and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination.</p>			<p>and</p> <p>(c) the number of subsequent law enforcement actions that were taken involving the use of PNR data [per air carrier and destination].</p>
	<p>23. These statistics shall not contain any personal data. They shall be transmitted to the Commission. On a yearly basis, <u>the Commission shall provide the Council with cumulative statistics referred to in Article 18(1).</u></p>			<p>3. On a yearly basis, the Commission shall provide the Council and the European Parliament with cumulative statistics referred to in Article 18(1).</p>

Article 19

Relationship to other instruments	Relationship to other instruments	Relationship to other instruments		Relationship to other instruments
<p>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.</p>	<p>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.</p>	<p>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.</p>		<p>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.</p>
		<p>1a. This Directive applies without prejudice to the Council Framework decision 2008 /977/JHA.</p>	<p>Art. also contained in DS 1576/15: <i>This Directive provides specific rules relating to the processing of personal data that either falls within the scope of the FD (exchanges between MSs) or to which the FD is made applicable (national processing). Thus, this Directive affects the FD. We suggest, instead, to clarify that Directive 95/46 remains applicable.</i></p>	<p>1a. This Directive is without prejudice to the applicability of Directive 95/46 to the processing of personal data by air carriers.</p>

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

Proposal for a revised list of offences

GA / ANNEX II

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. fraud, **including that against the financial interests of the EU,***
7. laundering of the proceeds of crime,* **money laundering and counterfeiting of currency, including the euro***
8. ~~computer-related crime~~ / **cybercrime***
9. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,*
10. ~~facilitation of unauthorised entry and residence,*~~ *? is this immigration related or those persons banned under risk to national / public security?*

murder, grievous bodily injury*

- 11. illicit trade in human organs and tissue,*
- 12. kidnapping, illegal restraint and hostage-taking,*
- 13. organised and armed robbery,*
- 14. ~~illicit trafficking in cultural goods, including antiques and works of art,*~~

counterfeiting and piracy of products,*

- 15. ~~forgery of administrative documents and trafficking therein,*~~ *Is this covered by 2?*
- 16. ~~illicit trafficking in hormonal substances and other growth promoters,*~~ *Is this not covered by trafficking in narcotics and psychotropic substances?*
- 17. illicit trafficking in nuclear or radioactive materials,*

rape

crimes within the jurisdiction of the International Criminal Court,

- 18. unlawful seizure of aircraft/ships,*
- 19. sabotage,*
- 20: trafficking in stolen vehicles,* **and industrial espionage.**

* = Europol mandate