EUROPEAN COMMISSION

Brussels, 2.2.2011
COM(2011) 32 final

2011/0023 (COD)

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

{SEC(2011) 132 final}
{SEC(2011) 133 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

Over the last decade the EU and other parts of the world have seen an increase in serious and organised crime, such as trafficking in human beings[1] and drugs[2]. According to the Sourcebook of Crime and Criminal Justice Statistics, there were approximately 14 000 criminal offences per 100 000 population in the EU Member States in 2007 (excluding Italy and Portugal for which data were not made available), ranging from 14 465 offences in Sweden to 958 in Cyprus. Europol's EU Organised Crime Threat Assessment 2009 (OCTA 2009), points out that most organised crime involves international travel, typically aimed at smuggling persons, drugs or other illicit goods into the EU.

At the same time, terrorists and terrorist organisations can be found both inside and outside the borders of the EU. The terrorist attacks in the United States in 2001, the aborted terrorist attack in August 2006 aimed at blowing up a number of aircraft on their way from the United Kingdom to the United States, and the attempted terrorist attack on board a flight from Amsterdam to Detroit in December 2009 showed the ability of terrorists to mount attacks, targeting international flights, in any country. While terrorism decreased in the EU during 2009, according to Europol's EU Terrorism Situation and Trend Report 2010, the threat of terrorism remains real and serious. Most terrorist activities are transnational in character and involve international travel[3], *inter alia* to training camps outside the EU, calling for increased cooperation between law enforcement authorities.

Serious crime and terrorist offences cause severe harm to victims, inflict economic damage on a large scale and undermine the sense of security without which persons cannot exercise their freedom and individual rights effectively.

A study published in 2009[4] for the International Labour Organisation estimated that the cost of coercion from underpayment of wages resulting from trafficking in human beings in 2007 in industrialised economies was $2 508 368 218, while the total for the world was $19 598 020 343.

The 2010 Annual report on the state of the drugs problem in Europe of the European Monitoring Centre for Drugs and Drug Addiction points to the global nature of the drugs problem and the growing and severe harm it entails. By undermining social development and feeding corruption and organised crime it represents a real threat for the European Union. Approximately 1 000 lives are lost in the EU annually due to cocaine-related deaths. The number of opioid users in Europe is cautiously estimated at 1.35 million. As regards the economic and social impacts of drugs, in 2008, 22 EU Member States reported a total expenditure relating to illicit drugs of EUR 4.2 billion.

---

1 Europol's EU Organised Crime Threat Assessment 2009

2 Eurostat 36/2009.

3 Europol's EU Terrorism Situation and Trend Report 2010

4 Measuring the costs of coercion to workers in forced labour- Vinogradova, De Cock, Belser.

Another study, from the UK Home Office[5], measured the costs incurred in anticipation of crime, such as defensive expenditure, the costs as a consequence of crime, such as the physical and emotional impact on the victim and the value of any property stolen and the costs incurred in response to crime, including the costs to the criminal justice system. These costs were measured at £ 36 166 000 000 in 2003.

In the meantime, four out of five Europeans wish to see stronger action at EU level against organised crime and terrorism[6].

As a response to the threat posed by serious crime and terrorism, and the abolition of internal border controls under the Schengen Convention, the EU adopted measures for the collection and exchange of personal data between law enforcement and other authorities. Although these measures have proven useful, they tend to focus on data relating to persons who are already suspected - i.e. persons who are "known" to law enforcement authorities. The Schengen Information System (SIS)[7] the second-generation Schengen Information System (SIS II)[8], the Visa Information System (VIS)[9], and the anticipated Entry/Exit System are examples of such measures.

In its 'Overview of information management in the area of freedom, security and justice'[10], the Commission provided an analysis of those measures and pointed to the need for increased cooperation between law enforcement authorities with respect to passengers on international flights to and from the Member States, including more systematic use of Passenger Name Record (PNR) data of such passengers for law enforcement purposes. The 'Stockholm Programme — An open and secure Europe serving and protecting the citizens'[11] also calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

PNR data is unverified information provided by passengers, and collected by and held in the carriers' reservation and departure control systems for their own commercial purposes. It contains several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent at which the flight was booked, means of payment used, seat number and baggage information.

Law enforcement authorities may use PNR data in several ways:

re-active: use in investigations, prosecutions, unravelling of networks after a crime has been committed. In order to allow law enforcement authorities to go back sufficiently in time, a commensurate period of retention of the data by law enforcement authorities is necessary;

real-time: use prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is

---

5 The economic and social costs of crime against individuals and households 2003/04.

6 Standard Eurobarometer 71, p. 149 of the Annex.

7 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19).

8 Regulation (EC) No 1987/2006, Decision 2007/533/JHA, Regulation (EC) No 1986/2006.

9 Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA. See also Declaration on combating terrorism, European Council, 25.3.2004.

10 COM(2010) 385.

11 Council document 17024/09, 2.12.2009.

being committed. In such cases PNR data are necessary for running against predetermined assessment criteria in order to identify previously 'unknown' suspects and for running against various databases of persons and objects sought;

pro-active: use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers. In order to carry out such an analysis of relevance for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, a commensurate period of retention of the data by law enforcement authorities is necessary.

More systematic collection, use and retention of PNR data with respect to international flights, subject to strict data protection guarantees, would strengthen the prevention, detection, investigation and prosecution of terrorist offences and serious crime and is, as further explained below, necessary to meet those threats to security and reduce the harm they cause.

The use of PNR data, however, is not currently regulated at EU level. Even though only a limited number of Member States have set up a PNR system to date, most Member States do use PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime in a non-systematic way or under general powers granted to the police or other authorities. Within the EU, the United Kingdom already has a PNR system, while France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation or are currently testing using PNR data. Several other Member States are considering setting up PNR systems. Those national measures diverge in several respects, including the purpose of the system, the period of data retention, the structure of the system, the geographic scope and the modes of transport covered. It is also very likely that once the complete regulatory framework on the use of PNR data in those Member States is adopted, there will be divergent rules on data protection and on the measures ensuring the security of data transfers. As a result, up to 27 considerably diverging systems could be created. That would result in uneven levels of protection of personal data across the EU, security gaps, increased costs and legal uncertainty for air carriers and passengers alike.

The proposal therefore aims to harmonise Member States' provisions on obligations for air carriers, operating flights between a third country and the territory of at least one Member State, to transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. It does not require air carriers to collect any additional information from passengers or to retain any data, nor does it require passengers to provide any data in addition to that already being provided to air carriers.

It is necessary to impose those legal obligations on air carriers for the following reasons.

First, PNR data enable law enforcement authorities to identify persons who were previously "unknown", i.e. persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved in such crime and who should therefore be subject to further examination by the competent authorities. Identifying such persons helps law enforcement authorities prevent and detect serious crimes including acts of terrorism. To achieve this, law enforcement authorities need to use PNR data both in real-time to run PNR against predetermined assessment criteria which indicate which previously 'unknown' persons require further examination and pro-actively for analysis and creation of assessment criteria.

For example, an analysis of PNR data may give indications on the most usual travel routes for trafficking people or drugs which can be made part of assessment criteria. By checking PNR data in real-time against such criteria, crimes may be prevented or detected. A concrete example given by a Member State is a case where PNR analysis uncovered a group of human traffickers always travelling on the same route. Using fake documents to check in for an internal flight, they would use authentic papers to simultaneously check in for another flight bound for a third country. Once in the airport lounge, they would board the internal flight. Without PNR it would have been impossible to unravel this human trafficking network.

The combined pro-active and real-time use of PNR data thus enable law enforcement authorities to address the threat of serious crime and terrorism from a different perspective than through the processing of other categories of personal data: as explained further below, the processing of personal data available to law enforcement authorities through existing and planned EU-level measures such as the Directive on Advance Passenger Information[12], the Schengen Information System (SIS) and the second-generation Schengen Information System (SIS II) do not enable law enforcement authorities to identify 'unknown' suspects in the way that the analysis of PNR data does.

Second, PNR data help law enforcement authorities prevent, detect, investigate and prosecute serious crimes, including acts of terrorism, after a crime has been committed. To achieve this, law enforcement authorities need to use PNR data in real-time to run the PNR data against various databases of 'known' persons and objects sought. They also need to use PNR data in a re-active manner to construct evidence and, where relevant, to find associates of criminals and unravel criminal networks.

For example, the credit card information which is part of the PNR data may enable law enforcement authorities to identify and prove links between a person and a known criminal or criminal organisation. An example given by a Member State relates to large scale human and drug trafficking involving a Member State and third countries. Cartels were importing drugs to several destinations in Europe. They were using drugs swallowers who were themselves trafficked persons. They were identified on the basis of having bought the ticket with stolen credit cards on the basis of PNR. This lead to arrests in the Member State. On this basis, an assessment criterion was created which itself led to several additional arrests in other Member States and third countries.

Finally, the use of PNR data prior to arrival allows law enforcement authorities to conduct an assessment and perform a closer screening only of those persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security. This facilitates the travel of all other passengers and reduces the risk of passengers being subjected to examination upon entry into the EU on the basis of unlawful criteria such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards.

The proposed measures entail the collection and processing of PNR data by law enforcement authorities and therefore has an impact on the rights to privacy and data protection. In order to ensure compliance with the principle of proportionality, the proposal is therefore, as explained further below, carefully limited in scope and contains strict data protection guarantees.

---

[12] Directive 2004/82/EC of 29 August 2004.

The necessity of using PNR data, in a limited manner and subject to strict data protection guarantees, is supported by a number of factual elements, as reflected in the Impact Assessment accompanying this proposal. In the absence of harmonised provisions on the collection and processing of PNR data at EU level, detailed statistics on the extent to which such data help prevent, detect, investigate and prosecute serious crime and terrorism are not available. The necessity of using PNR data is however supported by information from third countries as well as Member States that already use such PNR data for law enforcement purposes.

The experience of those countries shows that the use of PNR data has led to critical progress in the fight against in particular drugs, human trafficking and terrorism, and a better understanding of the composition and operations of terrorist and other criminal networks. With respect to drugs, Member States have indicated that the majority of seizures are made due to the use of PNR data in real-time and pro-actively. Belgium reported that 95% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data. Sweden reported that 65-75% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data. This represented 278.9 kilos of cocaine and additional quantities of heroin and other drugs. The United Kingdom reported that during a period of 6 months in 2010, 212 kilos of cocaine and 20 kilos of heroine were seized exclusively or predominantly due to the processing of PNR data.

- **General context**

On 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes[13] (hereinafter 'the 2007 proposal'). The proposal was extensively discussed in the Council working groups and the progress made in the discussions was endorsed by the Justice and Home Affairs Council in January, July and November 2008. The discussions on the proposal in the working groups allowed consensus to be reached on most of the provisions of the proposal[14].

Upon entry into force of the Treaty on the Functioning of the European Union (TFEU) on 1 December 2009, the Commission proposal, not yet adopted by the Council, became obsolete. The current proposal replaces the 2007 proposal and is based on the provisions of the TFEU. It takes into account the recommendations of the European Parliament as stated in its Resolution of November 2008[15] and it reflects the latest state of discussions in the Council working groups in 2009. It also takes into account the opinions of the European Data Protection Supervisor[16], the Article 29 Working Party on Data Protection[17] and the Fundamental Rights Agency[18].

- **Existing provisions in the area of the proposal**

PNR data are different from and should not be confused with Advance Passenger Information (API). API data are the biographical information taken from the machine-readable part of a

13 COM(2007) 654.
14 Council document 5618/2/09 REV 2, 29.6.2009.
15 P6_TA (2008)0561.
16 OJ C 110, 1.5.2008.
17 Opinion number 145 of 5.12.2007.
18 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf

passport and contain the name, place of birth and nationality of the person, the passport number and expiry date. Thus they are different and more limited in scope than PNR data.

In the EU, the use of API is regulated by the API Directive[19]. The Directive provides that API data should be made available to border control authorities, at the request of each Member State, for flights entering the territory of the EU for the purpose of improving border controls and combating irregular immigration. Even though their use for law enforcement purposes is permitted by the Directive, this is possible only if specific criteria are fulfilled. Thus, although API data are in some cases used by law enforcement authorities in order to identify suspects and persons sought, they are mainly used as an identity verification and border management tool. Moreover, API data do not enable law enforcement authorities to conduct an assessment of passengers, and therefore do not facilitate the detection of hitherto 'unknown' criminals or terrorists.

The **Schengen Information System** (SIS) seeks to maintain public security, including national security, within the Schengen area. SIS is a centralised information system comprising a national part in each participating state and a technical support function in France. Member States may issue alerts for persons wanted for arrest for extradition; aliens to be refused entry; missing persons; witnesses or those under judicial summons; persons and vehicles subject to additional checks; lost or stolen vehicles, documents and firearms; and suspect bank notes.

The **Visa Information System** (VIS) seeks to address both concerns: its purpose is to help implement a common visa policy by facilitating the examination of visa applications and external border checks while contributing to the prevention of threats to Member States' internal security. It is a centralised information system which comprises a national part in each participating state and a technical support function in France. VIS will use a Biometric Matching System to ensure reliable fingerprint comparisons, and will be deployed at EU external borders to verify the identity of visa-holders. It will include data on visa applications, photographs, fingerprints, related decisions of visa authorities and links between related applications.

Therefore, as with API, the SIS and the VIS are mainly used as identity verification and border management tools and are only useful where the identity of the suspect is known. These instruments are neither useful for conducting assessment of persons nor for detecting 'unknown' criminals or terrorists.

Agreements for the transfer of PNR data in the context of the fight against serious transnational crime and terrorism, limited to travel by air, have been signed between the EU and the United States, Canada and Australia. These require air carriers, collecting PNR data of passengers for their own commercial purposes, to transmit these data to the competent authorities of the United States, Canada and Australia. These three agreements are due to be renegotiated during 2011. Other countries, notably South Korea and Japan, have also requested to negotiate such agreements. The Commission has outlined the core elements of an EU policy in this area in its Communication of 21 September 2010 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries'[20]. The current proposal is fully coherent with the policy set out in that Communication.

---

19 Directive 2004/82/EC of 29 August 2004.

20 COM(2010) 492.

- **Consistency with the EU's other policies and objectives**

The Schengen Information System (SIS)[21] the second-generation Schengen Information System (SIS II)[22], the Visa Information System (VIS)[23], and the anticipated Entry/Exit System and Registered Travellers Programme are EU measures that deal directly with actions taking place physically at the borders.

Even though PNR are passenger data linked to travel, they are mainly used as a criminal intelligence tool rather than as a border control tool. They are used in advance of a border crossing and not at the border crossing itself. The main aim of using PNR data is to fight terrorism and serious crime rather than to fight irregular immigration and facilitate border controls.

The proposal will neither change nor interfere with current EU rules on the way border controls are carried out or with the EU rules regulating entry and exit from the territory of the Union. The proposal will rather co-exist with and leave those rules intact.

- **Impact on fundamental rights**

The proposal is fully in line with the overall objective of creating a European area of freedom, security and justice. Because of the nature of the proposed provisions, this proposal was subject to in-depth scrutiny to ensure that its provisions are compatible with fundamental rights, and especially the right to protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights of the EU, as reflected in the Impact Assessment accompanying this proposal. The proposal is also in line with Article 16 of the TFEU, which guarantees everyone the right to the protection of personal data.

The proposal is compatible with data protection principles and its provisions are in line with the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[24] ('Framework Decision 2008/977/JHA'). This includes giving individuals the right of access, the right of rectification, erasure and blocking, as well as the right to compensation and judicial redress. Furthermore, and in order to comply with the proportionality principle, there are areas where the proposal will have stricter rules on data protection than Framework Decision 2008/977/JHA.

In particular, the scope of the proposal is strictly limited and law enforcement authorities are allowed to use PNR data only for the purpose of combating an exhaustive list of specified serious crimes, which in addition has to be subject to a prison sentence of at least three years in the Member State. Moreover, in order to ensure that the processing of data of innocent and unsuspected persons remains as limited as possible, some aspects of the scope of the proposal relating to the creation and application of assessment criteria were further limited to serious crimes that are also transnational in nature, i.e. are intrinsically linked to travelling and hence the type of the data being processed. The proposal allows retention of PNR data for period of

---

21 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19).

22 Regulation (EC) No 1987/2006, Decision 2007/533/JHA, Regulation (EC) No 1986/2006.

23 Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA. See also Declaration on combating terrorism, European Council, 25.3.2004.

24 OJ L 350, 30.12.2008, p. 60.

time not exceeding 5 years, after which the data must be deleted. Moreover, the data must be anonymised after a very short period of 30 days since pro-active use of PNR data is possible on the basis of the anonymised data after this period of time. The collection and use of sensitive data directly or indirectly revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life, is prohibited. Moreover, the proposal provides that a decision taken by a Member State, producing adverse legal effects on a person or seriously affecting him/her, must not be taken on the basis of automated processing of PNR data only. Moreover such decision may under 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. Furthermore, carriers must transmit PNR data exclusively by the so-called "push" method, meaning that the Member States will not have direct access to the carriers' IT systems. PNR data may only be transferred by Member States to third countries in very limited circumstances and only on a case-by-case basis. In order to ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority (data protection authority) is responsible for advising and monitoring how PNR data are processed. Member States are also required to establish a single designated unit (Passenger Information Unit) responsible for handling and protecting the data. All processing of PNR data must be logged or documented by this Passenger Information Unit for the purpose of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of the data processing. Member States must also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.

Therefore, in addition to being in line with existing data protection rules and principles, the proposal contains a number of safeguards to ensure full compliance with the proportionality principle and guarantee a high level of fundamental rights protection.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

When preparing the 2007 proposal, the Commission consulted all stakeholders on the basis of a questionnaire in December 2006. The questionnaire was sent to all the Member States, the data protection authorities of the Member States, the European Data Protection Supervisor, the Association of European Airlines (AEA), the Air Transport Association of America (ATA), the International Air Carrier Association (IACA), the European Regions Airline Association (ERA) and the International Air Transport Association (IATA). The replies were summarised in the Impact Assessment which accompanied the 2007 proposal. Subsequently, the Commission invited the Member States to a meeting during which the representatives of the Member States had the opportunity to exchange views.

Following the adoption of the 2007 proposal, all stakeholders published their positions on it. The European Parliament adopted a resolution on the proposal on 20 November 2008[25]. The Member States expressed their positions through the discussions in the Council working

[25] P6_TA (2008)0561.

groups[26]. Opinions were also issued by the European Data Protection Supervisor[27], the Article 29 Data Protection Working Party[28] and the Fundamental Rights Agency[29].

Summary of responses

The main criticism expressed in the Resolution of the European Parliament was that the need for the proposed actions had not been sufficiently demonstrated. Parliament questioned whether the proposal met the standard required for justifying an interference with the right to data protection. The Resolution expressed Parliament's concern that the added value of the proposal in the light of other border initiatives had not been assessed. As regards data protection, Parliament called for a clear purpose limitation and emphasised that only specific authorities should have access to PNR data. Finally Parliament expressed concerns that the proposed method of automatically assessing PNR data using fact-based pre-determined assessment criteria was a very wide use of the data and stressed that such assessment should never result in 'profiling' on the basis of sensitive data.

The Article 29 Data Protection Working Party considered that the proposal was disproportionate and that it might violate the right to data protection. It called into question the data protection regime as Framework Decision 2008/977/JHA does not cover domestic processing of data. It considered that the demonstration of the need for the proposal was inadequate, that the data retention period (13 years) was disproportionate and that only the 'push' method of data transfer should be used.

The European Data Protection Supervisor questioned whether the necessity and proportionality of the proposal had been demonstrated since the proposal concerns the collection of data of innocent persons. He criticised the proposal as contributing towards a surveillance society and also called into question the data protection regime as domestic processing of data is not covered by Framework Decision 2008/977/JHA. The European Data Protection Supervisor specifically suggested better defining the authorities that would have access to PNR data and the conditions for transferring data to third countries.

The Fundamental Rights Agency was also of the opinion that the necessity and proportionality of the proposal had not been demonstrated and considered that there should be more guarantees in the proposal in order to avoid profiling on the basis of sensitive data.

Some airline associations, namely the International Air Transport Association (IATA) and the Association of European Airlines (AEA), also issued opinions on the proposal. These mainly criticised the decentralised structure of the proposal and stressed that centralised collection of the data would have financial advantages for the carriers. They also criticised the choice of the 'push' method and called for the choice of transfer method to be left to the carriers.

The consultation process has had a major impact on the legislative proposal. Even though several stakeholders were not convinced of the necessity of using PNR data, they all agreed that legislation at EU level is preferable to the development of diverging national PNR systems. The consultations also led to limitation of the purpose of using the data to the fight

---

26 Council document 17024/09, 2.12.2009.

27 OJ C 110, 1.5.2008.

28 Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007 (WP 145 of 5.12.2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_en.pdf.

29 http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.

against terrorist offences and serious crime and limitation of the scope of the proposal to air transport. A strong data protection regime was chosen with a specific retention period and prohibition of the use of sensitive data, such as data revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life. The 'push' method was preferred, as well as strict limitations on onward transfers of data to third countries.

- **Collection and use of expertise**

There was no need for external expertise.

- **Impact assessment**

The Commission carried out the Impact Assessment listed in the Work Programme[30].

Four main options were examined in the Impact Assessment, each containing two variables:

Policy Option A, refraining from addressing the issue at EU level and maintaining the status quo.

Policy Option B, addressing the structure of a system for collecting and processing PNR data, with option B.1: Decentralised collection and processing of data by Member States and option B.2: Centralised collection and processing of data at EU level.

Policy Option C, addressing limitation of the purpose of the proposed measures, with option C.1: Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime only and option C.2: Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and other policy objectives.

Policy Option D, addressing the modes of transport to be covered by the proposed measures, with option D.1: Air carriers only and option D.2: Air, sea and rail carriers.

The options were assessed against the following criteria: security in the EU, protection of personal data, costs to public authorities, costs for carriers/competition in the internal market and encouraging a global approach.

The Impact Assessment concluded that a legislative proposal applicable to travel by air with decentralised collection of PNR data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and other serious crime was the best policy option (combination of B1, C1 and D1). This would enhance security in the EU, while limiting the impact on the protection of personal data to the minimum and keeping costs at an acceptable level.

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposal aims to harmonise Member States' provisions on obligations for air carriers, operating flights between a third country and the territory of at least one Member State, to

[30] SEC(2011) 132.

transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. All processing of PNR data on the basis of this proposal will comply with the data protection rules laid down in Framework Decision 2008/977/JHA.

- **Legal basis**

The TFEU, and in particular Articles 82(1)(d) and 87(2)(a).

- **Subsidiarity principle**

Law enforcement authorities must be provided with effective tools with which to fight terrorism and serious crime. As most serious crimes and terrorist acts involve some international travel, authorities need to use PNR data to protect the internal security of the EU. Furthermore, investigations for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes carried out by the competent authorities of the Member States are largely dependent on international and cross-border cooperation.

Because of the free movement of persons in the Schengen area, it is necessary that all Member States collect, process and exchange PNR data, in order to avoid security gaps. By acting collectively and coherently, this measure will contribute to increasing the security of the EU.

Action at EU level will help to ensure harmonised provisions on safeguarding data protection in the Member States. The different systems of Member States that have already established similar mechanisms, or will do so in the future, may impact negatively on the air carriers as they may have to comply with several potentially diverging national requirements, for example regarding the types of information to be transmitted and the conditions under which this information needs to be provided to the Member States. These differences may also be prejudicial to effective cooperation between the Member States for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

Since the objectives of this proposal cannot be sufficiently achieved by the Member States, and can be better achieved at Union level, it can be concluded that the EU is both entitled to act and better placed to do so than the Member States acting independently. The proposal therefore complies with the subsidiarity principle as set out in Article 5 of the Treaty on European Union.

- **Proportionality principle**

The proposed systematic collection, analysis and retention of PNR data with respect to flights into the EU from third countries, subject to strict data protection guarantees, would strengthen the prevention, detection, investigation and prosecution of terrorist offences and serious crime and is necessary to meet those threats to security.

The scope of the proposal is limited to those elements that require a harmonised EU approach, including the definition of the ways in which PNR can be used by the Member States, the data elements that need to be collected, the purposes for which the information may be used, the communication of the data between the PNR units of the Member States, and the technical conditions for such communication.

The proposed action is a directive. The choice of a decentralised system means that the Member States can choose how they set up their PNR system, and can decide themselves on the technical aspects of it.

In accordance with the principle of proportionality, as set out in Article 5 of the Treaty on European Union, this proposal does not go beyond what is necessary and proportionate in order to achieve its objectives.

- **Choice of instrument**

Proposed instrument: a directive.

Other means would not be adequate for the following reason:

The aim of the measure is the approximation of Member States' legislation, so that any instrument other than a directive would not be appropriate.

4. BUDGETARY IMPLICATION

The proposal has no implication for the EU budget.

5. ADDITIONAL INFORMATION

- **Simulation, pilot phase and transitional period**

There will be a transitional period for the proposal in the form of a two year implementation period. There will also be a transitional collection of PNR data, aiming to achieve collection of data on all flights within 6 years from the entry into force of the Directive.

- **Territorial application**

The proposed Directive will be addressed to the Member States. Application of the Directive to the United Kingdom, Ireland and Denmark will be determined in accordance with the provisions of Protocols Nos 21 and 22 annexed to the Treaty on the Functioning of the European Union.

- **Review/revision/sunset clause**

The proposal includes a clause providing for a review of the operation of the Directive four years after its transposition date and a special review of the potential extension of the scope of the Directive to cover PNR data of passengers on flights internal to the EU.

2011/0023 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the Commission,

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

Having regard to the opinion of the European Economic and Social Committee[31],

Having regard to the opinion of the Committee of the Regions[32],

After having consulted the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) On 6 November 2007 the Commission adopted a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes[33]. However, upon entry into force of the Treaty of Lisbon on 1 December 2009, the Commission's proposal, which had not been adopted by the Council by that date, became obsolete.

(2) The 'Stockholm Programme — An open and secure Europe serving and protecting the citizens'[34] calls on the Commission to present a proposal for the use of PNR data to prevent, detect, investigate and prosecute terrorism and serious crime.

(3) In its Communication of 21 September 2010 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries'[35] the Commission outlined certain core elements of a Union policy in this area.

---

31 OJ C , , p. .
32 OJ C , , p. .
33 COM(2007) 654.
34 Council document 17024/09, 2.12.2009.
35 COM(2010) 492.

(4) Council Directive 2004/82/EC of 29 April 2004 on the obligation of air carriers to communicate passenger data[36] regulates the transfer of advance passenger information by air carriers to the competent national authorities for the purpose of improving border controls and combating irregular immigration.

(5) PNR data are necessary to effectively prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security.

(6) PNR data help law enforcement authorities prevent, detect, investigate and prosecute serious crimes, including acts of terrorism, 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.

(7) PNR data enable law enforcement authorities to identify persons who were previously "unknown", i.e. persons previously unsuspected of involvement in serious crime and terrorism, but whom an analysis of the data suggests may be involved in such crime and who should therefore be subject to further examination by the competent authorities. By using PNR data law enforcement authorities can address the threat of serious crime and terrorism from a different perspective than through the processing of other categories of personal data. However, in order to ensure that the processing of data of innocent and unsuspected persons remains as limited as possible, the aspects of the use of PNR data relating to the creation and application of assessment criteria should be further limited to serious crimes that are also transnational in nature, i.e. are intrinsically linked to travelling and hence the type of the data being processed.

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

(9) The use of PNR data together with Advance Passenger Information data in certain cases has added value in assisting Member States in verifying the identity of an individual and thus reinforcing their law enforcement value.

(10) To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is therefore essential that all Member States introduce provisions laying down obligations on air carriers operating international flights to or from the territory of the Member States of the European Union.

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

(12) The definition of terrorist offences should be taken from Articles 1 to 4 of Council Framework Decision 2002/475/JHA on combating terrorism[37]. The definition of serous crime should be taken from Article 2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender

---

[36] OJ L 261, 6.8.2004, p. 24.

[37] OJ L 164, 22.6.2002, p. 3. Decision as amended by Council Framework Decision 2008/919/JHA of 28 November 2008 (OJ L 330, 9.1.2.2008, p. 21).

procedure between Member States[38]. However, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality. The definition of serious transnational crime should be taken from Article 2 of Council Framework Decision 2002/584/JHA and the United Nations Convention on Transnational Organised Crime.

(13) PNR data should be transferred to a single designated unit (Passenger Information Unit) in the relevant Member State, so as to ensure clarity and reduce costs to air carriers.

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

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

(16) The Commission supports the International Civil Aviation Organisation (ICAO) guidelines on PNR. These guidelines should thus be the basis for adopting the supported data formats for transfers of PNR data by air carriers to Member States. This justifies that such supported data formats, as well as the relevant protocols applicable to the transfer of data from air carriers should be adopted in accordance with the advisory procedure foreseen in Regulation (EU) No….. of the European Parliament and the Council [……..]

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

---

[38] OJ L 190, 18.7.2002, p. 1.

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

(19) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or seriously affects him/her should be taken only by reason of the automated processing of PNR data. Moreover, no such decision should be taken by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.

(20) Member States should share with other Member States the PNR data that they receive where such transfer is necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime . The provisions of this Directive should be without prejudice to other Union instruments on the exchange of information between police and judicial authorities, including Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)[39] and Council Framework Decision 2006/960/JHA of 18 September 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[40]. Such exchange of PNR data between law enforcement and judicial authorities should be governed by the rules on police and judicial cooperation.

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

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

(23) The processing of PNR data domestically in each Member State by the Passenger Information Unit and by competent authorities should be subject to a standard of protection of personal data under their national law which is in line with Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[41] ('Framework Decision 2008/977/JHA').

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

---

39 OJ L 121, 15.5.2009, p. 37.
40 OJ L 386, 29.12.2006, p. 89.
41 OJ L 350, 30.12.2008, p. 60.

(25) Taking into account the right of passengers to be informed of the processing of their personal data, Member States should ensure they are provided with accurate information about the collection of PNR data and their transfer to the Passenger Information Unit.

(26) Transfers of PNR data by Member States to third countries should be permitted only on a case-by-case basis and in compliance with Framework Decision 2008/977/JHA. To ensure the protection of personal data, such transfers should be subject to additional requirements relating to the purpose of the transfer, the quality of the receiving authority and the safeguards applicable to the personal data transferred to the third country.

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

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

(29) As a result of the legal and technical differences between national provisions concerning the processing of personal data, including PNR, air carriers are and will be faced with different requirements regarding the types of information to be transmitted, as well as the conditions under which this information needs to be provided to competent national authorities. These differences may be prejudicial to effective cooperation between the competent national authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

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

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

(32) In particular, the scope of the Directive is as limited as possible, it allows retention of PNR data for period of time not exceeding 5 years, after which the data must be deleted, the data must be anonymised after a very short period, the collection and use

of sensitive data is prohibited. In order to ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority is responsible for advising and monitoring how PNR data are processed. All processing of PNR data must be logged or documented for the purpose of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of the data processing. Member States must also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.

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

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

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive provides for the transfer by air carriers of Passenger Name Record data of passengers of international 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.

2. The PNR data collected in accordance with this Directive may be processed only for the following purposes:

   (a) The prevention, detection, investigation and prosecution of terrorist offences and serious crime according to Article 4(2)(b) and (c); and

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

Article 2

Definitions

For the purposes of this Directive the following definitions shall apply:

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

(b) ‘international 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 final destination in a third country, including in both cases any transfer or transit flights;

(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 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;

(e) ‘reservation systems’ means the air carrier’s internal inventory 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 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;

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

(i) ‘serious 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 detention order for a maximum period of at least three years under the national law of a Member State, and if :

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

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

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

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

CHAPTER II

RESPONSIBILITES OF THE MEMBER STATES

Article 3

Passenger Information Unit

1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and 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.

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.

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.*

Article 4

Processing of PNR data

1. The PNR data transferred by the air carriers, pursuant to Article 6, in relation to international flights which land on or depart from the territory of each Member State shall be collected by the Passenger Information Unit of the relevant Member State. 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.

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 individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;

(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 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;

(c) responding, on a case-by-case basis, to duly reasoned 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 serious crime, and to provide the competent authorities with the results of such processing; and

(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).

3. The assessment of the passengers prior to their 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.

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.

Article 5

Competent authorities

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

2. Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime.

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*.

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.

5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

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

Article 6

Obligations on air carriers

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 Member States concerned.

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:

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

and

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

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.

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.

Article 7

Exchange of information between Member States

1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4(2)(a) and (b), the result of the processing of PNR data is transmitted by that Passenger Information Unit to the Passenger Information 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.

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).

3. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(2), and, if necessary, also the result of the processing of PNR data. The Passenger Information Unit may request access to specific PNR data kept by the Passenger Information Unit of another Member State in their full form without the masking out

only in exceptional circumstances in response to a specific threat or a specific investigation or prosecution related to terrorist offences or serious crime.

4. Only 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 other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.

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.

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.

Article 8

Transfer of data to third countries

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

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

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

Article 9

Period of data retention

1. Member States shall ensure that the PNR data provided by the air carriers to the Passenger Information Unit are retained in a database at the Passenger Information

Unit for a period of 30 days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.

2. Upon expiry of the 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 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.

   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:

   – 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.

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.

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.

Article 10

Penalties against air carriers

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

Article 11

Protection of personal data

1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to 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.

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 confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive

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.

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 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.

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 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.

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.

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 this Directive.

Article 12

National supervisory authority

Each Member State shall provide that the national supervisory authority established in implementation of Article 25 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.

CHAPTER IV

IMPLEMENTING MEASURES

Article 13

Common protocols and supported data formats

1. All transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made by electronic means or, 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.

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.

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).

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

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

Article 14

Committee procedure

1. The Commission shall be assisted by a committee ('the Committee'). That Committee shall be a committee within the meaning of Regulation […/2011/EU] of 16 February 2011.

2. Where reference is made to this paragraph, Article 4 of Regulation […/2011/EU] of 16 February 2011 shall apply.

CHAPTER V

FINAL PROVISIONS

Article 15

Transposition

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

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

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

Article 16

Transitional provisions

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

Article 6(1) are collected. Member States shall ensure that from four years after the date referred to in Article 15, the PNR data from all flights referred to in Article 6(1) are collected.

Article 17

Review

On the basis of information provided by the Member States, the Commission shall:

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

(b) undertake a review of the operation of this Directive and submit a report to the European Parliament and the Council within four years after the date mentioned in Article 15(1). Such review shall cover all the elements of this Directive, with special attention to the compliance with standard of protection of personal data, 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.

Article 18

Statistical data

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.

2. These statistics shall not contain any personal data. They shall be transmitted to the Commission on a yearly basis.

Article 19

Relationship to other instruments

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

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.

Article 20

Entry into force

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

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX

Passenger Name Record data as far as collected by air carriers

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name(s)

(5) Address and contact information (telephone number, e-mail address)

(6) All forms of payment information, including billing address

(7) Complete travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency/travel agent

(10) Travel status of passenger, including confirmations, check-in status, no show or go show information

(11) Split/divided PNR information

(12) General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

(13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any Advance Passenger Information (API) data collected

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