Basic information

2011/0023(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Directive	Procedure completed
Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime See also 2011/0126(NLE) See also 2011/0382(NLE) **Subject** 1.20.09 Protection of privacy and data protection 3.20.01.01 Air safety 7.10.04 External borders crossing and controls, visas 7.30 Police, judicial and customs cooperation in general 7.30.20 Action to combat terrorism 7.30.30 Action to combat crime	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs	KIRKHOPE Timothy (ECR)	15/07/2014

Former committee responsible	Former rapporteur	Appointed
LIBE Civil Liberties, Justice and Home Affairs		

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	DANJEAN Arnaud (PPE)	13/01/2015
TRAN Transport and Tourism	CRAMER Michael (Verts /ALE)	17/03/2015

Former committee for opinion	Former rapporteur for opinion	Appointed
AFET Foreign Affairs		
TRAN Transport and Tourism		

Council of the European Union

Council configuration	Meetings	Date
Justice and Home Affairs (JHA)	3433	2015-12-04
Justice and Home Affairs (JHA)	3162	2012-04-26
Justice and Home Affairs (JHA)	3354	2014-12-05
Justice and Home Affairs (JHA)	3081	2011-04-11
Justice and Home Affairs (JHA)	3415	2015-10-09

European Commission

Commission DG	Commissioner
Migration and Home Affairs	MALMSTRÖM Cecilia

Key events

Date	Event	Reference	Summary
02/02/2011	Legislative proposal published	COM(2011)0032	Summary
14/02/2011	Committee referral announced in Parliament, 1st reading		
11/04/2011	Debate in Council		Summary
26/04/2012	Debate in Council		Summary
29/04/2013	Committee report tabled for plenary, 1st reading	A7-0150/2013	Summary
10/06/2013	Decision by Parliament		Summary
20/10/2014	Committee referral announced in Parliament, 1st reading		
05/12/2014	Debate in Council		
15/07/2015	Vote in committee, 1st reading		
15/07/2015	Committee decision to open interinstitutional negotiations with report adopted in committee		
07/09/2015	Committee report tabled for plenary, 1st reading	A8-0248/2015	Summary
09/10/2015	Debate in Council		Summary
10/12/2015	Approval in committee of the text agreed at 1st reading interinstitutional negotiations		
13/04/2016	Debate in Parliament		
14/04/2016	Decision by Parliament, 1st reading	T8-0127/2016	Summary
14/04/2016	Results of vote in Parliament		
18/04/2016	Act adopted by Council after Parliament's 1st reading		
27/04/2016	Final act signed		
27/04/2016	End of procedure in Parliament		
04/05/2016	Final act published in Official Journal		

Technical information

Procedure reference	2011/0023(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
Amendments and repeals	See also 2011/0126(NLE) See also 2011/0382(NLE)
Legal basis	Treaty on the Functioning of the European Union TFEU 087-p2 Treaty on the Functioning of the European Union TFEU 082-p1
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/8/00066

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee report tabled for plenary, 1st reading/single reading		A7-0150/2013	29/04/2013	Summary
Committee draft report		PE549.223	17/02/2015	
Amendments tabled in committee		PE554.742	20/04/2015	
Amendments tabled in committee		PE554.743	20/04/2015	
Amendments tabled in committee		PE554.744	20/04/2015	
Committee opinion	TRAN	PE467.175	29/04/2015	
Committee opinion	AFET	PE549.344	06/05/2015	
Committee report tabled for plenary, 1st reading/single reading		A8-0248/2015	07/09/2015	Summary
Text adopted by Parliament, 1st reading/single reading		T8-0127/2016	14/04/2016	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00071/2015/LEX	27/04/2016	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2011)0032	02/02/2011	Summary
Document attached to the procedure	SEC(2011)0132	02/02/2011	
Document attached to the procedure	SEC(2011)0133	02/02/2011	

Commission response to text adopted in plenary	SP(2016)372	31/05/2016	
Follow-up document	SWD(2016)0426	28/11/2016	Summary
Follow-up document	COM(2020)0305	24/07/2020	
Follow-up document	SWD(2020)0128	24/07/2020	
Follow-up document	SWD(2021)0304	21/10/2021	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	DE_BUNDESRAT	COM(2011)0032	21/03/2011	
Contribution	RO_SENATE	COM(2011)0032	08/04/2011	
Contribution	IT_SENATE	COM(2011)0032	11/04/2011	
Contribution	BG_PARLIAMENT	COM(2011)0032	03/05/2011	
Contribution	CZ_SENATE	COM(2011)0032	27/05/2011	
Contribution	PT_PARLIAMENT	COM(2011)0032	02/08/2011	
Contribution	AT_NATIONALRAT	COM(2011)0032	31/07/2012	
Contribution	NL_SENATE	COM(2011)0032	15/04/2013	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EDPS	Document attached to the procedure	N7-0062/2011 OJ C 181 22.06.2011, p. 0024	25/03/2011	Summary
EESC	Economic and Social Committee: opinion, report	CES0803/2011	05/05/2011	
EDPS	Document attached to the procedure	N8-0115/2015 OJ C 392 25.11.2015, p. 0011	24/09/2015	Summary

Additional information

Source	Document	Date
National parliaments	IPEX	
European Commission	EUR-Lex	

Final act

Directive 2016/0681
OJ L 119 04.05.2016, p. 0132

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 26/04/2012

The Council agreed a **general approach** on a draft directive on the use of flight passenger data for protection against terrorist offences and serious crime (PNR data). The agreement among Member States on a general approach allows the Danish presidency to start negotiations with the European Parliament under the ordinary legislative procedure.

The discussion in the Council touched, among other things, on **two main issues**:

1) The first question concerned whether the proposed new rules should be limited to the collection of the Passenger Name Record (PNR) data for flights from and to third countries or whether flights within the EU should also be covered. **The proposed compromise would allow, but not oblige, Member States to collect PNR data also concerning selected intra-EU flights.**

2) The second question discussed was the retention period. The initial Commission proposal provides for a total retention period of five years. After 30 days, however, the PNR data would have to be masked out, so that the person-related elements of the PNR were no longer visible to the "front-desk" law enforcement officer, but can be seen only after a specific authorisation. A number of Member States considers that this initial storage period of 30 days is too short from an operational point of view. The **Council position agreed upon now is to maintain the overall retention period of five years but to prolong the first period during which the data are fully accessible to two years.**

The Council also adopted a decision on the conclusion of a new EU-US PNR agreement which will replace the existing one, provisionally applied since 2007. The European Parliament had given its consent on 19 April 2012. The agreement is expected to enter into force on 1 June 2012.

The aim of the agreement is to set up a legal framework for the transfer of PNR data by carriers operating passenger flights between the European Union and the United States to the US Department of Homeland Security (DHS) and the subsequent use of that data by the US DHS. The goal is to prevent, detect, investigate and prosecute terrorist offenses and related crimes as well as other serious cross-border crimes punishable by a sentence of imprisonment of at least three years.

The main aspects of the new PNR agreement with the US are:

- a **strict purpose limitation**, the use of PNR data being limited to the prevention, detection, investigation and prosecution of terrorist offences or transnational crime;
- a **legally binding commitment** from the US Department of Homeland Security to inform the Member States and EU authorities of any EU relevant intelligence leads flowing from the analysis of these PNR data;
- a robust data protection regime with strong data security and integrity requirements;
- rights of access, rectification and erasure and the possibility to obtain administrative and judicial redress;
- a limited usage of PNR data for a period of ten years for transnational crime and 15 years for terrorism. After 6 months personally identifiable information of PNR data will be masked out and after five years PNR data will be moved to a dormant database with additional controls.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 11/04/2011

Ministers examined a Commission proposal for a directive on the use of flight passenger data for protection against terrorist offences and serious crime.

One of the main questions discussed was whether the proposed new rules should be limited to the collection of the so-called Passenger Name Record (PNR) data for flights from and to third countries or whether flights within the EU should also be covered. **A majority of Member States was in favour of including at least an option so that each Member State can mandate the collection of such data also with regard to targeted intra-European flights**.

The overall purpose of the proposed directive is to set up a coherent EU-wide system on flight passenger data, by creating a single EU model for all Member States participating in the new rules and ensuring cooperation between the relevant authorities within the Union. As a consequence, all air carriers flying on routes covered by the new rules would need to provide PNR data to Member States' law enforcement authorities. These authorities will, however, only be allowed to use the data - that is already today collected by air carriers - for the prevention, detection, investigation and prosecution of terrorist offences and serious (transnational) crime.

24 EU Member States will certainly participate in the adoption of the new directive, while Denmark will not be bound by the new rules. As far as the UK and Ireland are concerned, they will need to give notification as to whether they want to opt-in or not.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 02/02/2011 - Legislative proposal

PURPOSE: to provide a legal framework on the on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

PROPOSED ACT: Directive of the European Parliament and of the Council.

BACKGROUND: the European Commission adopted, on Tuesday 6 November, a proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. This proposal has been subject to in-depth discussions with the Working Groups in the Council and the "Justice and Home Affairs" Council reviewed, in January, July and November 2008, the work carried out on this issue. The discussions enable a **consensus to be reached on many of the provisions**.

Following the entry into force of the Treaty on the Functioning of the European Union (TFEU) on the 1 December 2009, the 2007 draft framework proposal, which had not yet been adopted by the Council, became obsolete. This new proposal replaces it and is based on the provisions of the TFEU. It takes into account the views expressed by Member States in Council discussions on the draft Framework decision, as well as the recommendations of the European Parliament as stated in its Resolution of 20 November 2008 and the opinion of the European Data Protection Supervisor.

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 and drugs. This proposal responds to a request for increased cooperation on organised crime and terrorism. 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 such as the Schengen Information System (SIS) the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), and the anticipated Entry/Exit System are examples of such measures. The 'Stockholm Programme' 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. 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 necessary to meet those threats to security and reduce the harm they cause.

Given that the use of PNR data is not currently regulated at EU level, it is necessary 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. The proposal 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.

In order to ensure compliance with the principle of proportionality, the proposal is therefore carefully limited in scope and contains strict data protection guarantees.

IMPACT ASSESSMENT: four main options were examined in the Impact Assessment, each containing two variables:

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

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;
- with option B.2: Centralised collection and processing of data at EU level.

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;
- with option C.2: Access for the prevention, detection, investigation and prosecution of terrorist offences and serious crime and other policy objectives.

Option D: addressing the modes of transport to be covered by the proposed measures:

- with option D.1: Air carriers only;
- with 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.

LEGAL BASIS: Articles 82(1)(d) and 87(2)(a) of the Treaty on the Functioning of the European Union (TFEU).

CONTENT: the draft Directive contains several chapters which may be summarised as follows:

Chapter I - General provisions: 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 transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. The proposal is compatible with data protection principles and its provisions are in line with the Council Framework Decision 2008/977/JHA.

Passenger Name Record data as set out in the annex of the proposal include, inter alia:PNR record locator; date of reservation/issue of ticket; date(s) of intended travel; name(s); addresses; billing information; seat numbers; etc. Other general remarks are also made including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, 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).

Chapter II - Responsibilities:

On Member States: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. The PNR data transferred by the air carriers 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. Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities. 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.

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 for the purpose of further examination to the relevant **competent authorities** of the same Member State. Such transfers shall only be made on a case-by- case basis.

Obligations on air carriers:Member States shall adopt the necessary measures to ensure that air carriers transfer ('push') the PNR data 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. Air carriers shall transfer PNR data by electronic means using the **common protocols and supported data formats** to be adopted, 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.

Member States may permit air carriers to limit the transfer to updates of the transfers. 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 is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime.

Transfer of data to third countries: it is explicitly stated that a Member State may transfer PNR data to a third country under strict and limited conditions and with express authorisation from the Member States for the purpose of the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Period of data retention: 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. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit, 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**. Access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit 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 where it could be reasonably believed that it is necessary to carry out an investigation or prosecution.

Penalties against air carriers: 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.

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.

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 draft Decision lays down a number of provisions which aim to:

- prohibit 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;

- ensure the traceability of 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;
- 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;
- lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Directive.

Chapter IV - Implementing measures: this chapter concerns **common protocols and supported data formats**. 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. The technical provisions of comitology are also provided to this effect.

Chapter V - Final provisions: 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. 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.

The proposal includes a **review 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. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units.

Territorial application: the 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.

BUDGETARY IMPLICATION: this proposal has no implication for the EU budget.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 25/03/2011 - Document attached to the procedure

Opinion of the European Data Protection Supervisor on the 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 EDPS welcomes the fact that he was consulted by the Commission. Already before the adoption of the Proposal, the EDPS was given the possibility to give informal comments. Some of these comments have been taken into account in the Proposal, and the EDPS notes that globally speaking data protections safeguards in the Proposal have been strengthened. Remaining concerns are however still present on a number of issues, especially in relation to the **scale and purposes of the collection of personal data**.

The main purpose of an EU PNR scheme is the establishment of a system obliging air carriers operating international flights between the EU and third countries to transmit PNR data of all passengers to competent authorities, for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes. Data would be centralised and analysed by Passenger Information Units and the result of the analysis would be transmitted to competent national authorities in each Member State.

Since 2007, the EDPS has been following closely the developments related to a possible EU PNR scheme, in parallel with developments regarding PNR schemes of third countries. The main issue consistently raised by the EDPS focuses on the **justification of the necessity of a European PNR scheme** on top of a number of other instruments allowing for the processing of personal data for law enforcement purposes.

The EDPS acknowledges the visible improvements in terms of data protection in the present Proposal, compared to the version on which he has previously advised (see CNS/2007/0237). These improvements relate in particular to the scope of application of the Proposal, the definition of the role of different stakeholders (Passenger Information Units), the exclusion of the processing of sensitive data, the move towards a ‘push’ system without a transition period, and the limitation of data retention.

However, while there is a clear will to clarify the necessity of the scheme, **the EDPS still fails to find in these new justifications a convincing basis to develop the system, especially with regard to large scale ‘prior assessment' of all passengers**.

The EDPS is obliged to observe that the essential prerequisite to any development of a PNR scheme — i.e. compliance with necessity and proportionality principles — is not met in the Proposal. The EDPS recalls that in his view, PNR data could certainly be necessary for law enforcement purposes in specific cases and meet data protection requirements. It is the**ir use in a systematic and indiscriminate way**, with regard to all passengers, which raises specific concerns.

In the view of the EDPS, the only measure compliant with data protection requirements would be the use of PNR-data on **a case-by-case basis**, when there is a serious threat established by concrete indicators.

In addition to this fundamental shortcoming, the comments of the EDPS concern the following aspects:

- the scope of application should be much more limited with regard to the type of crimes involved. The EDPS questions the inclusion in the Proposal of serious crimes which have no link with terrorism. In any case, minor crimes should be explicitly defined and ruled out. **The EDPS recommends excluding the possibility for Member States to widen the scope of application**;
- the nature of the different threats allowing for exchange of data between PIUs or with Member States has not sufficiently been defined;
- the data protection principles applicable should not only rely on Council Framework Decision 2008/977/JHA which includes shortcomings, notably in terms of data subjects' rights and transfers to third countries. A higher standard of safeguards, based on the principles of Directive 95/46/EC, should be developed in the Proposal;
- **no data should be kept beyond 30 days in an identifiable form**, except in cases warranting further investigation;
- **the list of PNR data to be processed should be reduced**, in particular, the 'general remarks' field should not be included;
- the evaluation of the Directive should be based on comprehensive data, including the number of persons effectively convicted — and not only prosecuted — on the basis of the processing of their data.

The EDPS further recommends that the developments on EU PNR are assessed in a broader perspective including the ongoing general evaluation of all EU instruments in the field of information exchange management launched by the Commission in January 2010. In particular, the results of the current work on the European Information Exchange Model expected for 2012 should be taken into consideration in the assessment of the need for an EU PNR scheme.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 07/09/2015 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the second report by Timothy KIRKHOPE (ECR, UK) on the 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 committee recommended that the position of the European Parliament adopted in first reading following the ordinary legislative procedure should amend the Commission proposal as follows:

Purpose and scope: the purpose of the Directive is to ensure security, to protect the life and safety of the public, and to create a legal framework for the protection and exchange of PNR data between Member States and law enforcement authorities. The Directive provides for the transfer **by air carriers and non-carrier economic operators**, such as travel agencies and tour 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, and its exchange between Member States and between the Member States and Europol.

Offences covered: the amended rules state that PNR data may be processed only for the purposes of prevention, detection, investigation and prosecution of **terrorist offences and of certain types of serious transnational crime.** The list approved by Members includes, for example, trafficking in human beings, child pornography, drug trafficking, trafficking in weapons, munitions and explosives, cybercrime and money laundering.

The definition of **terrorist offences** is taken from Council Framework Decision 2002/475/JHA, including individuals who may be travelling for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training.

Passenger Information Unit: the 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;
- the exchange of PNR data and of the result of the processing thereof with the Passenger Information Units of other Member States and with Europol.

Member States' Passenger Information Units would be entitled to process PNR data **only for limited purposes**, such as identifying a passenger who may be involved in a terrorist offence or serious transnational crime and who requires further examination. They would appoint a **data protection officer** to monitor data processing and safeguards and act as a single contact point for passengers with PNR data concerns.

Processing of PNR data: the application of the Directive must be duly justified and the **necessary safeguards** must be in place in order to ensure the lawfulness of any storage, analysis, transfer and use of PNR data.

In carrying out an assessment of the risk presented by a passenger, the Passenger Information Unit may **compare PNR data against the Schengen Information System and the Visa Information System.**

Passenger assessment criteria must be **targeted, specific, justified, proportionate and fact-based**. They must 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.

Member States should also ensure that passengers are clearly and precisely informed about the **type of personal data** collected for law enforcement purposes and their rights.

Data retention period and masking out: PNR data transferred by air carriers and non-carriers would be retained in the national PIU for an initial period of 30 days, after which all data elements which could serve to identify a passenger would have to be **masked out**, and then for up to five years.

The masked out data would be accessible for up to **four years** in serious transnational crime cases and **five years** for terrorism ones.

After the five years, PNR data would have to be **permanently deleted**, unless the competent authorities are using it for specific criminal investigations or prosecutions (in which case the retention of data would be regulated by the national law of the Member State concerned).

Member States shall bear the costs of use, retention and exchange of PNR data. 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.

Conditions for Europol to access PNR data: 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.

Exchange of information shall take place by way of **SIENA** and in accordance with Decision 2009/371/JHA.

Protection of personal data: the Passenger Information Units shall maintain: (i) **documentation** of all processing systems and procedures under their responsibility; (ii) ensure a **high level of securit**y appropriate to the risks represented by the processing and the nature of the PNR data to be protected; (iii) inform the person concerned by his or her **rights** and the arrangements for exercising these rights.

Passenger Information Unit must keep **records** of at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. The persons who operate security controls, access and analyse the PNR data, and operate the data logs, shall be **security cleared and security trained**.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 14/04/2016 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 461 votes to 179 with 9 abstentions, a legislative resolution on the 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 position of the European Parliament adopted in first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Purpose and scope: the purpose of the Directive is to ensure security, to protect the life and safety of the public, and to create a legal framework for the protection and exchange of PNR data between Member States and law enforcement authorities. It provides for:

- the **transfer by air carriers** of passenger name record (PNR) data of passengers of **extra-EU flights**,
- the **processing of the data**, including its collection, use and retention by Member States and its exchange between Member States .

PNR data collected may be processed **only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime**.

Where an extra-EU flight has one or more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to the PIUs of all the Member States concerned.

If a **Member State decides to apply this Directive to intra-EU flights** (i.e. flying from one Member State to another Member States, without any stop-overs in the territory of a third country), it shall notify the Commission in writing.

Passenger information unit: each Member State shall establish an authority competent to act as its passenger information unit ('PIU'), responsible for:

- collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities;
- exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with **Europol**.

Data protection officer in the PIU: the PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards. A data subject must have the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.

Processing of PNR data: the PIU may only process data for carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities, and, where relevant, by Europol, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

When carrying out this assessment, the PIU may: (i) **compare PNR data against databases** relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases ; or (ii) process PNR data against pre-determined criteria.

The data protection officer must have access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority. The storage, processing and analysis of PNR data by the PIU shall be carried out exclusively within a secure location or locations within the territory of the Member States.

The consequences of the assessments of passengers **shall not jeopardise the right of entry of persons enjoying the Union right of free movement** into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council.

Conditions for access to PNR data by Europol: the amended text states that Europol may submit, on a case-by-case basis, an electronic and **duly reasoned request to the PIU** of any Member State through the Europol National Unit for the transmission of specific PNR data or the result of processing those data. Europol may submit such a request when this is **strictly necessary** to support and strengthen action by Member States to prevent, detect or investigate a specific terrorist offence or serious crime.

Transfer of data to third countries: transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances and only if:(a) such transfers are essential to respond to a specific and actual threat related to terrorist offences or serious crime in a Member State or a third country, and (b) prior consent cannot be obtained in good time.

Period of data retention and depersonalisation: PNR data provided by the air carriers to the PIU must be retained in a database at the PIU for a **period of five years** after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.

Upon expiry of a period of **six months** after the transfer of the PNR data, all PNR data shall be **depersonalised through masking out the data elements which could serve to identify directly the passenger to whom the PNR data relate**, such as name, address and contact information, and all forms of payment information, including billing address, and frequent flyer information.

Upon expiry of the period of **six months**, disclosure of the full PNR data **shall be permitted only where** it is:(a) reasonably believed that it is necessary and (b) approved by either a judicial authority, or another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an ex-post review by that data protection officer.

Protection of personal data: the amended text states that the PIUs must maintain documentation relating to all processing systems and procedures under their responsibility. **Processing must not be based** on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. The PIU must keep **records** of at least the following processing operations: collection, consultation, disclosure and erasure. The records of consultation and disclosure shall show, in particular, the purpose, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed the PNR data and the identity of recipients of those data. Those records shall be kept for a period of **five years**.

Review: the Commission shall conduct a review of all the elements of the Directive **four years** after the date of entry into force of the latter. It shall pay special attention to: compliance with the applicable standards of protection of personal data, the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, the length of the data retention period, and the effectiveness of exchange of information between Member States.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 28/11/2016 - Follow-up document

This Commission document presents the **implementation plan** for Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Member States are required to transpose the Directive into national legislation by **25 May 2018**.

The experience of both Member States and non-EU countries that have a functional PNR system in place or are in advanced stages of its finalisation illustrates the **challenges**, in terms of **resources, time and technical complexity**, of setting up PNR systems compliant with the Directive. This process requires (i) fully establishing and equipping the national Passenger Information Units (PIUs), (ii) testing the operation of their IT systems and (iii) making the necessary adjustments to ensure the system operates properly.

National measures required for the implementation of Directive (EU) 2016/681: the Commission identifies the most important measures that Member States introduce as being to:

- provide a legal basis for the collection and processing of PNR data that includes all the data protection safeguards provided for in the Directive **and in the horizontal provisions applicable**, in particular those of Directive (EU) 2016/6803 which will need to be transposed, except in exceptional circumstances, by 6 May 2018, i.e. before the deadline for transposition of the EU PNR Directive. In particular, Member States should consider providing for a **clear indication of the databases against which PNR data may be compared** (Art 6(3)(a)) and the main principles governing the creation, update and operation of the predetermined criteria against which PNR are processed (Art 6(3)(b) and (4);
- identify and **designate the national authority or authorities** that will host the PIU and how the latter will be incorporated in their administrative structure;
- equip the PIU with the required **technical infrastructure** allowing for the storage, processing and analysis of PNR data;
- train the PIU personnel in order to be able to perform its duties of **effectively analysing PNR data** for law enforcement purposes;
- identify and designate the **competent authorities entitled to request and receive PNR data** or the result of processing those data from the PIU;
- inform **air carriers** of the technical specifications concerning the transfer of PNR data and the necessary tests that must be conducted to ensure their **connectivity** with the technical infrastructure of the PIU;
- devise appropriate solutions to ensure that the PIUs are able to **exchange PNR data effectively and in a timely manner**.

Member States' progress towards implementation: the state of the Directive's implementation varies greatly across Member States. A number of them already either have a functional PNR system in place or are in advanced stages of its finalisation.

- currently, four Member States have both functional or almost functional PNR systems in place and a dedicated legal basis providing for the collection or processing of PNR data; amendments are however still needed to fully adjust the legislative framework to the requirements of the Directive; the experience of these four Member States provides **best practice examples** that should be used by other Member States;
- twelve Member States are in various stages of completion of the technical infrastructure and of the adoption of a dedicated PNR legislation;
- eleven Member States are still at a relatively early stage of the implementation process, with the concrete acquisition and development of the technical infrastructure yet to start. However, some of these Member States have already devised detailed implementation plans with concrete deadlines.

Support actions: to support and follow Member States' progress in implementing the PNR Directive, the Commission is taking the following actions:

- **regular meetings with Member States and Europol** to discuss legal questions linked to the interpretation and implementation of the Directive and to share queries, lessons learnt, and best practices ;
- **financial assistance to Member States:** the Commission has proposed to the budgetary authority to provide an additional amount of EUR 70 million to assist Member States in setting up their PIUs. This additional funding would be allocated mainly through Internal Security Fund national programmes and possibly also using Union Actions. Discussions with Member States on the practical details for benefiting from this funding will be held in due course. The Commission stands ready to provide further financial support if necessary;
- **Commission implementing decision on data formats and transmission protocols:** this decision provides a list of common protocols and supported data formats to be used by air carriers when transferring PNR data to the PIUs.

Possible Member State actions: the Commission has identified a number of **indicative milestones** that Member States should meet in order to have their PIUs up and running by May 2018. They cover aspects such as:

- ensuring the enacting legislation is compliant with the Directive;
- setting up PIUs;
- setting in place technical solutions for the processing of PNR data;
- staffing of PIUs;
- involvement of competent authorities (e.g. identifying the competent authorities entitled to request or receive PNR data);
- ensuring carrier connectivity.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 29/04/2013 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted, by a slight majority (30 votes to 25, with no abstentions) the report by Timothy KIRKHOPE (ECR, UK) on the 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 committee recommends that the European Parliament should **reject** the Commission proposal. It calls on the Commission to withdraw its proposal.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 27/04/2016 - Final act

PURPOSE: to provide for the transfer by air carriers of PNR data and the processing of the data for the purposes of detecting, preventing, investigating and prosecuting terrorist offences and serious crime.

LEGISLATIVE ACT: Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

CONTENT: the Directive aims to **regulate the transfer to the EU, by air carriers, of passenger name record (PNR) data of passengers of extra-EU flights** , and the processing of such data by competent authorities.

If a Member State decides to apply the Directive to **intra-EU flights**, it shall notify the Commission in writing. A Member State may also 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 pursue the objectives of the Directive.

Passenger information unit (PIU): to ensure efficiency and a high level of data protection, Member States are required to ensure that an **independent national supervisory authority** and, in particular, a **data protection officer** are responsible for advising and monitoring the way PNR data are processed.

- A data subject must have the **right to contact the data protection officer**, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.
- **The data protection officer** must have access to all data processed by the PIU, and if he considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority.

- **Europol** may submit, on a case-by-case basis, an electronic and duly reasoned request to the PIU of any Member State through the Europol National Unit for the transmission of specific PNR data or the result of processing those data.

Processing of data: PNR data gathered may only be used for the purposes of detecting, preventing, investigating and prosecuting terrorist offences and serious crime.

Accordingly, the PIU shall process PNR data only for carrying out an **assessment of passengers prior to their scheduled arrival in or departure** from the Member State. The assessment may only be carried out to identify persons who require further examination by the competent authorities, and, where relevant, by Europol, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

When carrying out the assessment, the PIU may: (a) compare PNR data against relevant databases; (b) process PNR data against **pre-determined criteria**.

Any assessment of passengers against pre-determined criteria shall be carried out in a **non-discriminatory** manner. Those pre-determined criteria must be targeted, proportionate and specific.

Transfer of data to third countries: a Member State may transfer PNR data to a third country, only on a case-by-case basis and in full compliance with the provisions laid down by Member States pursuant to Framework Decision 2008/977/JHA. Transfers of PNR data without prior consent of the Member State from which the data were obtained shall be permitted in exceptional circumstances.

Period of data retention and depersonalisation: the Directive provides for the retention of PNR data in the PIUs for a period of time **not exceeding five years**, after which the data should be deleted. It provides for the data to be depersonalised after an **initial period of six months**, through **masking out** of data elements which could serve to identify directly the passenger to whom the PNR data relate, such as name, address, and contact information, and also all forms of payment information, including billing address, and frequent flyer information.

Upon expiry of the period of six months, disclosure of the full PNR data shall be permitted only under strictly defined circumstances.

Protection of personal data: all processing of PNR data should be **logged or documented** for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. The PIU must keep **records** of at least the following processing operations: collection, consultation, disclosure and erasure. Those records shall be kept for a period of **five years.**

The Directive **prohibits the processing of sensitive PNR data** revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.

Common protocols and supported data formats: as of one year after the date the Commission first adopts common protocols and supported data formats in accordance with paragraph 3, all transfers of PNR data by air carriers to the PIUs for the purposes of this Directive shall be made electronically using secure methods conforming to those common protocols.

ENTRY INTO FORCE: 24.5.2016.

TRANSPOSITION: 25.5.2018.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 09/10/2015

The presidency informed the Council on the work progress on the proposal for a directive on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

To recall, in April 2012 the Justice and Home Affairs Council agreed on a general approach regarding the draft directive.

The Council and the European Council have regularly highlighted the urgency of finalising this directive, in light of the growing threat posed by foreign fighters.

On 15 July 2015, the committee in charge of the proposal at the European Parliament adopted a revised report on the directive and a mandate to open negotiations with the Council.

Negotiations between the institutions on the draft directive are ongoing.

Use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

2011/0023(COD) - 24/09/2015 - Document attached to the procedure

Second Opinion of the European Data Protection Supervisor (EDPS) on the 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 (PNR Directive).

To recall, the legislative procedure has been in abeyance since the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) **rejected the Proposal on 24 April 2013**, questioning its necessity and proportionality. Recently, the discussions have been revived following the terrorist attacks that took place in Paris in January 2015.

In its Resolution of 11 February 2015 on anti-terrorism measures, the European Parliament committed itself **to work towards the finalisation of an EU PNR Directive by the end of the year.** It also:

- urged the Commission to set out the consequences of the ECJ judgment on the Data Retention Directive and its possible impact on the EU PNR Directive;
- called on the Member States to make optimal use of existing platforms, databases and alert systems at European level, such as the Schengen Information System (SIS) and the Advanced Passenger Information Systems (APIS);
- encouraged better exchange of information between Member States' law enforcement authorities and EU agencies.

The European Parliament also encouraged the Council to **make progress on the Data Protection Package** so that the 'trilogue' negotiations on both the EU PNR Directive and the Data Protection Package could take place in parallel.

In this context, an **updated report** has been presented by the rapporteur for the LIBE Committee, on 17 February 2015. Several modifications to the Commission proposal were proposed in this document, such as the inclusion of intra-EU flights. The LIBE Committee adopted its orientation vote on 15 July 2015 and agreed to enter into negotiations with the Council.

This EDPS Opinion will address the **changes in the Proposal as proposed by the LIBE Committee and the Council in view of the trilogue negotiations** that are due to begin in November 2015.

The EDPS welcomed the various improvements made by the Council and the LIBE Committee on the Proposal, for example regarding the specific provisions on data protection, the presence of a Data Protection Officer, or a specific reference to the power of the supervisory authorities.

However, the **essential prerequisite for a PNR scheme — i.e. compliance with necessity and proportionality principles — is still not met in the Proposal**.

The EDPS notes that:

- the proposal does not provide for a comprehensive evaluation of the ability of the current existing instruments to reach the purpose of the EU PNR scheme;
- it does not set forth any detailed analysis of the extent to which less intrusive measures could achieve the purpose of the EU PNR scheme;
- the **non-targeted and bulk collection and processing of data** of the PNR scheme amount to a measure of general surveillance.

In the view of the EDPS, the only purpose which would be compliant with the requirements of transparency and proportionality, would be the **use of PNR data on a case-by-case basis but only in case of a serious and concrete threat** established by more specific indicators.

It is for this reason that **the EDPS encourages the legislators to further explore the feasibility against current threats of more selective and less intrusive surveillance measures** based on more specific initiatives focusing, where appropriate, on targeted categories of flights, passengers or countries.

The EDPS considered that:

- the Proposal should limit the data retention period to what is justified by objective criteria explaining the period retained;
- the proposal should more explicitly provide that the PNR data may not be used for other purposes than the prevention, detection, investigation or prosecution of terrorist offences and serious transnational crimes;
- a prior approval by a court or an independent administrative body should be obtained, in principle, upon a request of access to the data by a competent authority;
- the Proposal should refer to appropriate safeguards guaranteeing the security of the data processed by the PIU;
- the scope of the PNR scheme should be much more limited with regards to the type of crime;
- the criteria required to access PNR data by the competent authorities should be better defined and more precise.

The EDPS invited the legislators to wait until the adoption of the new Data Protection Package to fully align the obligations of the Proposal with the new provisions adopted. Moreover, the evaluation of the Directive should be based on comprehensive data, including the number of persons effectively convicted and not only prosecuted, on the basis of the processing of their data.