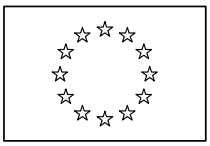

EUROPEAN COMMISSION

Brussels, 21.9.2010
COM(2010) 492 final

COMMUNICATION FROM THE COMMISSION

On the global approach to transfers of Passenger Name Record (PNR) data to third countries

COMMUNICATION FROM THE COMMISSION

On the global approach to transfers of Passenger Name Record (PNR) data to third countries

1. INTRODUCTION

The terrorist attacks in the United States in 2001, in Madrid in 2004 and in London in 2005 led to a new approach to internal security policies. Recent events like the attempted terrorist attack on an airplane on Christmas Day in 2009 and in Times Square, New York in 2010 indicate that the terrorist threat is still with us. At the same time, organised crime, especially drugs and human trafficking, is increasing[1].

As a response to these continuing threats, the EU and other third countries adopted new measures, which included the collection and exchange of personal data. An overview of these measures has been provided by the Commission in its Overview of information management in the area of freedom, security and justice[2]. The use of Passenger Name Record (PNR) data for law enforcement purposes is one such measure.

On 16 January 2003 the Commission issued a Communication to the Council and the Parliament on the Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach[3] aimed at setting out the elements of a global EU approach on PNR. The Communication called for a legally secure framework for PNR transfers to the US Department of Homeland Security and the adoption of an internal policy on PNR. It also called for the development of the push system of transfers of data by the air carriers[4] and an international initiative on PNR data transfers by International Civil Aviation Organisation (ICAO).

The conclusions of that Communication have been implemented to a large extent, while others are in the process of being implemented. Namely, the EU signed an agreement with the U.S. Department of Homeland Security for the transfer of PNR data in the interest of the fight against terrorism and serious transnational crime and which ensures transfer of PNR data whilst providing for the protection of personal data[5]. In addition the Commission adopted a proposal for a Framework Decision for the use of PNR data for law enforcement purposes[6]. The Commission is currently examining, on the basis of an impact assessment, the possibility of replacing it with a proposal for a Directive on the use of PNR data for law enforcement purposes. The push system of transfers of data has been adequately developed by most carriers while ICAO developed a series of guidelines for PNR transfers to governments.

In addition to the agreement with the US, the EU signed similar agreements with Canada[7] and Australia[8]. New Zealand, South Korea and Japan are also using PNR data but until the date of this report, have not entered into agreements with the EU. Within the EU, the United

---

1 Eurostat 36/2009.
2 COM(2010) 385.
3 COM(2003) 826.
4 The 'push' system entails that the carrier transmits the data to the third country, rather than the carrier allowing access to its databases by a third country.
5 OJ L 204, 4.8.2007, p. 16.
6 COM(2007) 654.
7 OJ L 91, 29.3.2006, p. 53, OJ L 91, 29.3.2006, p. 49 and OJ L 82, 21.3.2006, p. 15.
8 OJ L 213, 8.8.2008 p. 49.

Kingdom has a PNR system in place, while other Member States have either enacted the relevant legislation or are testing using PNR data.

These developments indicate that the use of PNR data is growing and is increasingly seen as a mainstream and necessary aspect of law enforcement work. At the same time, the use of PNR data involves the processing of personal data which raises important issues with respect to the fundamental rights to the protection of private life and to the protection of personal data.

As a result, the EU is faced with new challenges as regards international PNR transfers. The number of countries in the world developing PNR systems will most likely increase in the coming years. Furthermore, the EU gained important insight into the structure and value of PNR systems through its experience with carrying out joint reviews of the agreements with US and Canada.

The Commission therefore deems it necessary to re-consider its global approach to transfers of PNR data to third countries. The revision of this approach should ensure strong data protection guarantees and full respect of fundamental rights, and be in line with the principles of policy development which have been defined in the Overview of information management in the area of freedom, security and justice[9]. The views on general PNR issues of the major stakeholders, like the Member States, the European Parliament, the European Data Protection Supervisor and the Article 29 Data Protection Working Party, are especially important in the development of the revised approach on PNR.

The key objective of this communication is to establish, for the first time, a set of general criteria which should form the basis of future negotiations on PNR agreements with third countries. This will assist the EU in dealing with the current trends, while also serving as a method to communicate to third countries, to Member States and to citizens how the European Commission wishes to define its external PNR policy. Recommendations by the Commission for negotiations of PNR agreements with third countries should in the future respect, at a minimum, the general criteria established in the Communication, while additional criteria could be set in each recommendation.

2. INTERNATIONAL TRENDS ON PNR

2.1. PNR data and its use

PNR data is unverified information provided by passengers and collected by carriers for enabling reservations and carrying out the check-in process. It is a record of each passenger's travel requirements held in carriers' reservation and departure control systems. It contains several different types of information, for example dates of travel and travel itinerary, ticket information, contact details like address and phone numbers, travel agent, payment information, seat number and baggage information.

PNR data are different from Advance Passenger Information (API). API data are the biographical information taken from the machine-readable part of a passport and contain the name, place of residence, place of birth and nationality of a person. Under the API Directive[10], API data are made available to border control authorities only for flights entering the territory of the EU for the purpose of improving border controls and combating illegal immigration. Even though their use for other law enforcement purposes is permitted by the Directive, this is thought to be an exception rather than a rule. They are held by Member States for 24 hours.

---

9 COM(2010) 385.

10 Directive 2004/82/EC of 29.8.2004 on the obligation of carriers to communicate passenger data.

API data are mainly used to carry out identity checks as part of border controls and border management, although in some cases the data is also used by law enforcement authorities in order to identify suspects and persons sought. API data are thus primarily used as an identity management tool. The use of such data is becoming increasingly common around the world with more than 30 countries using it systematically, while more than 40 are in the process of setting up API systems.

In addition to the transmission of API data, some countries require carriers to transmit to them PNR data. Such data are then used in the fight against terrorism and serious crime, such as trafficking in human beings and drugs. PNR have been used for almost 60 years mainly by Customs authorities but also law enforcement authorities around the world. However, until recently now, it was not technologically possible to access such data electronically and in advance, so their use was limited to manual processing of only some flights. The technological advances today make the advance electronic transmission of the data possible.

The uses of PNR data are very different from those of API data, largely due to the fact that a PNR contains very different types of data. PNR are mainly used as a criminal intelligence tool rather than as an identity verification tool. The uses of PNR are mainly the following: (i) risk assessment of passengers and identification of "unknown" persons, i.e. persons that might potentially be of interest to law enforcement authorities and who were so far unsuspected, (ii) earlier availability than API data, and provision of an advantage to law enforcement authorities in allowing more time for its processing, analysis and any follow-up action, (iii) identification to which persons specific addresses, credit cards etc that are connected to criminal offences belong, and (iv) matching of PNR against other PNR for the identification of associates of suspects, for example by finding who travels together.

PNR data are unique in their nature and their use. Such use can be:

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

real time (present data): use in order to prevent a crime, survey or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR are necessary for running against predetermined fact-based risk indicators in order to identify the previously "unknown" suspects and for running against various databases of persons and objects sought.

pro-active (patterns): use for trend analysis and creation of fact-based travel and general behaviour patterns, which can then be used in real time use. In order to establish travel and behaviour patterns, trend analysts need to be allowed to use the data over a sufficiently long period of time. A commensurate period of retention of the data by law enforcement authorities is necessary in such cases.

2.2. Current trends

Some third countries, i.e. the United States, Canada, Australia, New Zealand and South Korea, are already using PNR data for law enforcement purposes. Other third countries have either enacted relevant legislation and/or are currently testing using PNR data, i.e. Japan, Saudi Arabia, South Africa and Singapore. Several other third countries started considering the idea of using PNR, but have not yet enacted relevant legislation. Within the EU, the UK already has a PNR system. France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation and/or are currently testing using PNR data. Several other Member States are considering setting up PNR systems.

The European Commission, recognising the necessity of PNR data for the prevention and fight against terrorism and serious crime, and in line with the 2003 Communication, tabled a proposal for a Framework Decision on the use of passenger name record (PNR) data for law enforcement purposes. As a result of the entry into force of the Treaty of Lisbon, the Commission is considering replacing this proposal with a proposal for a Directive for the use of PNR data for law enforcement purposes. The proposal will aim to oblige air carriers to transmit PNR data to the Member States to be used in the fight against terrorist offences and serious crime.

It is increasingly accepted on an international level that PNR are a necessary tool in the fight against terrorism and serious crime. This trend is the result of three parameters. First, international terrorism and crime are a serious threat to society and steps need to be taken to deal with these problems. The access to and analysis of PNR data is one such step that is considered necessary from a law enforcement perspective. Second, recent technological developments have rendered such access and analysis possible, which was inconceivable some years ago. The various technological developments of recent years are also widely used by criminals in the planning, preparation and execution of crimes. And lastly, with the rapid increase of international travel and the volume of passengers, the electronic processing of data in advance of the arrival of passengers largely facilitates and expedites security and border control checks since the risk assessment process is done before arrival. It provides the opportunity to law enforcement to focus only on those passengers for whom they have a fact-based reason to believe that they might pose an actual risk to security, rather than making assessments based on instinct, pre-conceived stereotypes or profiles.

2.3. Effects of the current trends on the European Union

The data protection laws of the EU do not allow carriers operating flights from the EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data without adducing appropriate safeguards. As a result, when the United States, Canada and Australia requested carriers to transmit PNR data for flights to their countries, the carriers were faced with a very difficult situation. The EU therefore stepped in and negotiated and signed separate international agreements with each of these three countries[11], thus making the transfer of PNR data outside of the EU to law enforcement authorities of these third countries possible. This was done in order to help carriers out of this situation, to ensure an adequate level of protection of the data of passengers and as recognition of the necessity and importance of the use of PNR data in the fight against terrorism and serious crime.

As more countries implement PNR systems, it is expected that the same issue will continue to arise. In addition, if the Commission decides to proceed with a proposal for an EU PNR Directive, the frequency of such requests may intensify if third countries ask for reciprocity from the EU.

Until today, the conclusion of international agreements with third countries on PNR was "demand" driven and dealt with on a case-by-case basis. Even though all the agreements address common issues and regulate the same matters, their provisions are not identical. This sometimes resulted in diverging rules for carriers and for data protection. As the "demand" is

---

[11] 2004 EC-US PNR agreement (OJ L 183, 20.5.2004, p. 84) and Commission Decision of 14 May 2004 (OJ L 235, 6.7.2004, p. 11); 2006 EU-US PNR agreement (OJ L 298, 27.10.2006, p. 29) and accompanying letters (OJ C 259, 27.10.2006, p. 1), 2007 EU-US PNR agreement (OJ L 204, 4.8.2007, p. 18), EU-Canada PNR Agreement (OJ L 82, 21.3.2006, p. 15 and OJ L 91, 29.3.2006, p. 49) and EU-Australia PNR Agreement (OJ L 213, 8.8.2008, p. 47).

likely to increase in the near future, a strategy could assist the EU in facing these demands in a more structured manner, leading to less divergence between the various agreements.

3. A REVISED GLOBAL APPROACH ON PNR FOR THE EU

3.1. Reasons underlying a revised global approach on PNR

At a time when the conclusions of the 2003 Communication are being implemented and where the EU is faced with new trends and challenges, it is important that the EU takes due account of those trends and challenges by further developing its global approach in relation to the transfer of PNR data to third countries for the following reasons:

Fight against terrorism and serious transnational crime: the EU has an obligation to itself and to third countries to cooperate with them in the fight against these threats. One way of such cooperation is the exchange of data with third countries. Making PNR data available for law enforcement purposes is a necessary means to fighting terrorism and serious transnational crime. Both the Strategy for the External Dimension of Justice and Home Affairs[12], as well as the EU Counter-Terrorism Strategy[13] and the Stockholm Programme[14] mention such a need for close cooperation with third countries.

Ensure the protection of personal data and privacy: the EU is committed to ensure a high level and effective protection of personal data, including that any transmission of PNR data to third countries is done in a secure manner in line with existing EU legal requirements and that passengers are able to enforce their rights in relation to the processing of their data.

Need to provide legal certainty and streamline the obligations on air carriers: it is important that the EU provides a coherent legal framework for the transmission of PNR data by air carriers to third countries. This is necessary in order to protect carriers from sanctions and to ensure that the conditions and modalities governing the transmissions of data world-wide are as uniform and harmonised as possible in order to reduce the cost burden on the industry and to ensure a level-playing field in the sector.

Establish general conditions aimed at ensuring coherence and further developing an international approach: the agreements that the EU has signed with third countries on PNR are similar as to the purpose but their contents vary as regards the modalities of the transmissions and the nature of the commitments of the third country. Such divergence in the commitments is acceptable to some degree in view of different requirements and different legal orders in each country, but all should respect certain general criteria (see sections 3.2 and 3.3 below). In the interest of ensuring an as uniform as possible treatment of passengers and reducing the costs on the industry, it is important that the content and standards of future agreements with third countries are as similar as possible. This could then form the basis for the next step, which could consist of a more harmonised multilateral approach to exchanges of PNR data.

Contribution in increasing passenger convenience: in order to deal with the security threats that are present in our societies, the checks of passengers upon crossing a border are becoming more detailed and lengthier. This, coupled with the ongoing increase of the volume of international travel, lead to the creation of longer waiting times at the borders. The advance electronic transmission of PNR before the crossing of a border makes it possible to check

---

12 COM(2005) 491.

13 Council document 14469/4/05 of 30.11.2005.

14 Council Document no.17024/09 of 2.12.2009.

passengers in advance, which enables them to cross borders quicker and more easily, while it permits law enforcement authorities to focus only on the identified persons of interest.

3.2. General considerations

The revised global approach on PNR aims to provide the basis for the EU to decide how to best deal with requests from third countries for the transmission of PNR data in the future. In addition to the principles of policy development which have been defined in the Overview of information management in the area of freedom, security and justice the following specific considerations arerelevant:

Shared security interest: Terrorism and serious crime are international in nature. Certain countries of the world are more exposed to the increasing threats of terrorism and serious crime than others. The EU is committed to cooperate with them and assist in combating these security threats.

Protection of personal data: Since the transmission, use and processing of PNR data affects the fundamental right of individuals to protection of their personal data, it is of central importance that the EU only cooperates with those third countries that can provide an adequate level of data protection for the EU originating PNR data.

External relations: the overall external relationship of the EU with the third country should also be considered. The functioning of and cooperation with the police and the judiciary, rule of law and the overall respect of fundamental rights are important factors to be considered.

3.3. Standards, content and criteria

The global PNR approach should outline the general standards that international agreements between the EU and third countries should meet so as to achieve as much coherence as possible with respect to the data protection guarantees to be applied by those countries and to the modalities of the transmissions of the data by the air carriers.

It is also essential that the EU is provided with mechanisms for monitoring the correct implementation, for example through regular joint review of the implementation of the agreements, and effective dispute resolution mechanisms.

3.3.1. Protection of personal data

The collection and transfer of PNR data to third countries affects a very large number of individuals and their personal data. Thus, particular attention must be paid to the effective protection of personal data.

In Europe, the fundamental rights to respect for private life and to protection of personal data are enshrined in Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the EU[15]. These fundamental rights apply to every person regardless of nationality or place of residence. Further standards for data protection have been set in the Council of Europe Convention 108 of 1981 on the Protection

[15] It is important to note that similar data protection principles have been laid down in international instruments regarding the protection of privacy and personal data, such as: Art. 17 of the International Covenant on Civil and Political Rights of 16. December 1966, the UN Guidelines for the Regulation of Computerized Personal Data Files (UN General Assembly Resolution 45/95 of 14 December 1990), the Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data, and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and the Additional Protocol to that Convention (ETS No. 181), which are also open to adhesion for non-European States.

of Individuals with regard to automatic processing of personal data and its additional Protocol 181 of 2001.

Any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of these rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Since data protection regimes in third countries can differ from the data protection prevailing in the EU, it is important that for any transfer of PNR data from EU Member States to third countries, the third country ensures an adequate level of data protection based on a sound legal basis. Such an adequate level of data protection can be either enshrined in the legislation of the third country or be provided in the form of legally binding commitments in the international agreement governing the processing of personal data.

The adequacy afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation. In this context, the EU will also consider the compliance by the third country with international standards, respectively its ratification of international instruments on data protection and fundamental rights in general. Adequacy decisions already adopted by the European Commission in this regard should be used as guidance on what can be regarded as being adequate.

The basic principles for the protection of personal data that the requesting third country should apply are the following:

- **Purpose limitation – use of data:** The scope of the use of the data by a third country should be spelt out clearly and precisely in the agreement and should be no wider than what is necessary in view of the aims to be achieved. Experience with current PNR agreements shows that PNR data should be used only for law enforcement and security purposes to fight terrorism and serious transnational crime. Key notions like terrorism and serious transnational crime should be defined based on the approach of definitions laid down in relevant EU instruments.
- **Purpose limitation – scope of data:** The exchange of data should be limited to the minimum and should be proportionate. Any agreement should list exhaustively the categories of PNR data to be transferred.
- **Special Categories of Personal Data (sensitive data):** PNR data revealing racial or ethnic origins, political opinions or religious or philosophical beliefs, trade union membership, health or sexual life shall not be used unless under exceptional circumstances where there is an imminent threat to loss of life and provided that the third country provides appropriate safeguards, for example that such data may be used only on a case-by-case basis, under the authorisation of a high-ranking official and strictly limited to the purposes of the original transfer.
- **Data Security:** PNR data must be protected against misuse and unlawful access by all appropriate technical, security procedures and measures to guard against risks to the security, confidentially or integrity of the data.
- **Oversight and accountability:** A system of supervision by an independent public authority responsible for data protection with effective powers of intervention and enforcement shall exist to exercise oversight over those public authorities that use PNR data. The latter shall be accountable for complying with the established rules on the

protection of personal data, and should have powers to hear complaints from individuals concerning the processing of PNR data.

- **Transparency and Notice:** Every individual shall be informed at least as to the purpose of processing of personal data, who will be processing that data, under what rules or laws, the types of third parties to whom data is disclosed and how and from whom redress can be sought.
- **Access, rectification and deletion:** Every individual shall be provided with access to his or her PNR data as well as, where appropriate, the right to seek rectification and deletion of his or her PNR data.
- **Redress:** Every individual shall have the right to effective administrative and judicial redress where his or her privacy has been infringed or data protection rules have been violated, on a non discriminatory basis regardless of nationality or place of residence. Any such infringement or violation shall be subject to appropriate and effective sanctions and/or remedies.
- **Automated Individual Decisions:** Decisions producing adverse actions or effects on an individual may not be based solely on the automated processing of personal data without human involvement.
- **Retention of data:** the period of retention of the PNR data should not be longer than necessary for the performance of the defined tasks. The period of retention should take into account the different ways in which PNR data are used (see section 1.2.1 above) and the possibilities of limiting access rights over the period of retention, for example by gradual anonymisation of the data.
- **Restrictions on onward transfers to other government authorities:** PNR data should only be disclosed to other government authorities with powers in the fight against terrorism and serious transnational crime, and which afford the same protections as those afforded by the recipient agency under the agreement in accordance with an undertaking to the latter. PNR data should never be disclosed in bulk but only on a case-by-case basis.
- **Restrictions on onward transfers to third countries:** this considers primarily restrictions on use and further dissemination in order to avoid circumvention of the agreement when PNR data is made available to another third country. Such onward transfers shall be subject to appropriate safeguards. In particular, the receiving third country should transfer this information to a competent authority of another third country only if the latter undertakes to treat the data with the same level of protection as set out in the agreement and the transfer is strictly limited to the purposes of the original transfer of the data. PNR data should never be disclosed in bulk but only on a case-by-case basis**.**

3.3.2. Modalities of transmissions

In order to provide legal certainty and minimise the financial burden on the air carriers, it is important to streamline the rules governing the transmission of the data by the carriers to third countries. By having uniform obligations, the financial burden on the carriers would be greatly reduced as they would have to undertake less investment to comply with their obligations. For this purpose, it would be desirable if at least the following modalities of transmissions were standardised:

- **The method of transmission**: To safeguard the data that is contained in the carriers' databases and to maintain their control thereof, data should be transmitted using exclusively the 'push' system.

- **The frequency of transmission**. There should be a reasonable limit to the number of times that the third country requires the data to be transmitted to it, which ensures an adequate benefit to security while minimising the costs of the carriers.
- **No obligation on the carriers to collect additional dat**a. The carriers should not be required to collect any more data than they already do or to mandatorily collect certain types of data, but only be required to transmit what they already collect as part of their business.

3.3.3. Overarching concepts

- **Duration and review:** The terms of the cooperation with third countries should be valid for a fixed duration and should provide the possibility that either party denounces the agreement. It should be possible to review the terms of the cooperation where it is considered appropriate.
- **Monitoring:** It is essential that the EU is provided with mechanisms for monitoring the correct implementation, for example through periodical joint reviews on the implementation of all aspects of the agreements, including the purpose limitation, the rights of passengers and onward transfers of PNR data, and comprising a proportionality assessment of the retained data on the basis of their value to achieving the purposes for which the data were transferred. The findings of such joint reviews should be presented to the Council and the European Parliament.
- **Dispute resolution**: Effective dispute resolution mechanisms with respect to interpretation, application and implementation of agreements should be provided.
- **Reciprocity:** reciprocity should be ensured, especially through the transfer of analytical information flowing from PNR data by competent authorities of the receiving third country to police and judicial authorities of the Member States, as well as to Europol and Eurojust.

4. LONGER TERM PERSPECTIVE

As more and more countries in the world use PNR data, the issues arising from such use affect the international community. Even though the bilateral approach which has been adopted by the EU was the most appropriate one under the circumstances and seems to be the most appropriate one for the near future, it risks ceasing to be appropriate if many more countries become involved with PNR. The EU should therefore examine the possibility of setting standards for the transmission and use of PNR data on an international level. The Guidelines on PNR access that have been developed by ICAO in 2004 offer a solid basis for the harmonisation of the modalities of transmissions of PNR data. However, these guidelines are not binding and they deal insufficiently with data protection issues. They are therefore not sufficient in themselves, but should rather be used for guidance, especially on matters affecting the carriers.

On this basis, the EU should therefore consider initiating discussions with international partners that use PNR data and those that are considering such use, in order to explore whether there is common ground between them for dealing with PNR transfers on a multilateral level. In case that these discussions are successful, the EU should enter into formal negotiations with the interested international partners to achieve a multilateral solution.

5. CONCLUSION

This Communication provided an overview of the current trends in the use of PNR data in the EU and the world. As a response to those trends, as well as the threats that the EU and the world continue to face, the Commission considered it necessary for the EU to review its global approach on PNR. In doing so, the Commission has taken account of the views on general PNR issues of the major stakeholders and the principles of policy development set out in the Overview of information management in the area of freedom, security and justice.

This Communication lays down, for the first time, a series of general considerations which should guide the EU in negotiating PNR agreements with third countries. Adherence to those principles should lead to greater coherence between the various PNR agreements, whilst ensuring respect for the fundamental rights to respect for private life and to protection of personal data. At the same time, the Communication remains sufficiently flexible and adaptable to each third country's particular security concerns and national legal order.

Finally, looking at the longer term perspective in the development of PNR policies worldwide, this Communication concludes that the EU should explore the possibility of replacing, in the medium term, bilateral agreements by a multilateral agreement between all countries that use PNR data.