PROTECTION OF PASSENGER NAME RECORDS DATA IN GREECE AFTER THE OLYMPIC GAMES EXPERIENCE

PRESENTATION

By Ioannis THEMELIS
Lawyer – Researcher on European Law

International Seminar in the University of Nijmegen
15 – 16 march 2007, the Netherlands

Index:

I. INTRODUCTION

Ladies and Gentlemen,

In the aftermath of the terrorist attacks of 11 September 2001, the United States passed legislation in November 2001, requiring that air carriers operating flights to, from or through the United States provide the United States' Customs with electronic access to the data contained in their automated reservation and departure control systems, known as Passenger Name Records (PNR). A **Passenger Name Record** (**PNR**) is the travel record for a person (or small group of persons) as used by airline and travel agency databases. Colloquially, "PNR" may also refer to the unique six-character record locator used to identify the record. From a technical point, there are five parts of a PNR required before the booking can be completed. They are:

- The name of the passenger(s).
- Contact details for the travel agent or airline office.
- Ticketing details, either a ticket number or a ticketing time limit.
- Itinerary of at least one sector, which must be the same for all passengers listed..
- Name of the person making the booking.

While the above list is the minimum requirement, there is a considerable amount of other information required by both the airlines and the travel agent to ensure efficient travel. These include,

- Fare details, and any restrictions that may apply to the ticket.
- The form of payment used, as this will usually restrict any refund if the ticket is not used.
- Further contact details, such as phone contact numbers at their home address and intended destination.
- Age details if it is relevant to the travel, eg, unaccompanied children or elderly passengers requiring assistance.
- Details of special meal requirements, seating preferences, and other similar requests.

In more recent times, many governments now require further information to be included to assist investigators tracing criminals or terrorists. These requirements give rise to some of the privacy concerns listed below. These include,

- Passengers' full names. (Prior to 9/11, most airlines only used an initial letter and family name).

- Passport details- nationality, number, and date of expiry.
- Date and place of birth.

The entire list you can find and see in page 10.

The structure of my paper was based in two levels: in one hand, I exanimate the European agreement to transfer the PNR in third non-EU countries like USA, and in other, my analysis is based on the Greek legal and political reality during and after the Olympic Games of 2004 in Athens. Finally, I expose my conclusions.

II. EUROPEAN PROTECTION OF PNR

In general frame, the data protection of individuals and the crossborder exchange of these informations in EU level has become the focus of discussions within Europe. In 24 October 1995 EU adopt a directive, the directive 95/46/EC in aim to creating a high and harmonized data protection standard for all Members States. This Directive enshrines two of the oldest ambitions of the European integration project: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important.

As response in the demand to the transfer of the European Passenger Name Records Data by the States, this directive offers two strong arguments that oppose in the satisfaction of this request.

First, the Directive prohibits, in general, any transfer of personal data to "third countries" (non-EU countries) if these countries do not provide an adequate level of data protection. Article 25 clarifies the definition of an "adequate level" of safeguards. The US is considered such a third country, since it does not offer any safeguards for the protection of personal data equivalent to the one provided by the Directive.[1] Thus, even if one may argue that the requested transfer were compatible with the contractual purpose of the airlines (relying on the argument that, without the transmission, the airlines would simply not be able to carry their passenger to the US), the transfer would generally be prohibited, because of the US' lack of adequate safeguards. This prohibition could only be circumvented when the airlines get an "unambiguous" consent from their passenger for this specific disclosure (see Article 26). This means, pursuant to the Directive, a "freely given specific and informed indication of a person's wish." The information provided to the

[1] see: Working Party's Opinion 1/99

data subject must include the identity of the US Agency, the purpose of this request and a notification that the data will be transferred to a country that does not offer adequate privacy safeguards (Articles 10 und 11 of the Directive).

And second, there are narrowly interpreted exemptions, such as in Article 13 of the directive 95/46/EC. Article 13 stipulates that the European Member States may restrict the scope of the obligations in the mentioned articles when such a restriction constitutes a necessary measure to safeguard national security, defense, public security, prosecution of criminal offences or other purposes not related to the US request.[2] The words "necessary measure" make it clear that these exemptions are restricted only for specific investigations. Therefore, the exemption rule of Article 13 cannot justifiably be invoked to restrict the obligations of the Directive where the transfer is systematic as it is foreseen by the US Customs. Since Article 13 requires a case by case request, the systematic general US request does not comply with it.

---

[2] see: Article 29 Working Party's Opinion Nr. 66 of October 24, 2002 (pdf)

For the history, two Decisions, one by the EU Conseil and the other by the EU Commission take place in May 2004. The Decision by the EU Conseil of treatment and deliverance of PNR at US Authorities 2004/496/EC and Decision by the EU Commission of treatment and deliverance of PNR at US Authorities 2004/535/E. The European Community and the United States signed an International Agreement on 28 May 2004 that makes possible the transfer of air passenger data to the US, under certain conditions. It entered into force with immediate effect. This agreement goes hand-in-hand with the Decision adopted two weeks ago by the European Commission, establishing the adequacy of US Bureau of Customs and Border Protection's personal data protection.

Then the EU Parliament realizes two Demands at the European Court for the annulation of this accord. On 21 April 2004, the European Parliament decided to ask the European Court of Justice for an opinion on whether the Agreement was compatible with the Treaty of the European Community. In the meantime the agreement has been concluded. Furthermore, on 25 June 2004, the European Parliament chose to bring an action for annulment of the international agreement, in accordance with Article 230 of the EC Treaty.

Finally, EU Court's decision annulled this accord in 30 may 2006 for technical reasons (because of the EU Parliament was in the march of the procedure without be demanded his opinion on this issue - and not by jugging the substance of this accord). So, following this application by the European Parliament, the Court of Justice of the European Communities (ECJ) annulled the Commission's adequacy decision and the Council decision concerning the conclusion of this international agreement while preserving the effect of the decision on adequacy until 30 September 2006. Therefore the international agreement remained in force until end of September latest.

III. GREEK PROTECTION OF PNR

Why this accord was important for Greece?

a) DURING OLYMPIC GAMES

In 2004 Greece was the host country of the Olympic games in Athens. A number of international agreements between Greece and other countries such as USA were have been taken place unilaterally, without asking the previous agreement of the European Communities, in order to prevent international (Al Quida) and domestic (local revolutionary extreme-left terrorism) terrorist acts. Greece has also a number of efficacy specific laws for the adequate protection of the personal data mentioned in the paper, including the article 9

of the Greek Constitution of the Republic. More precisely, the article 9 recognize the right of individual to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. Among them the most important is the Law 2472/1997 who was introduced, incorporating Directive 95/46/EC into Greek law, and establishing the Hellenic Data Protection Authority.

In Article 5 of Law no. 2472/97 it is probably necessary to get consent when is not impracticable or inappropriate, unless in "exceptional" circumstances. As "exceptional" circumstances may be consider as the reasons of the protection of public order and issues of reserves of national safeguard national security, defense, public security, prosecution of criminal offences or other purposes. For this reasons the Greek State has the right to have access in the individual's personal data and use them for reasons of national interest.

In Article 9 of Law no. 2472/97 the transfer of personal data such as PNR to a country that is not member of the EU can be succeeded by permission that can provide the State's Aythorities in condition (article 11) to inform the individual about the finalities and the contain of the information that are providing before the act of transfer.

That practically means that during, and after as it proved, the Olympic Games in Athens, Greek State had the authority of treating not only the PNR but also and other sensitive personal data as transfer them to third countries, including USA, in aim to protect the national and international – delegation of athletes from all over the world – security!

b) SPECIAL LAWS

More precisely, by the decision 67/2004 by the Hellenic Data Protection Authority the Greek State had the right, as according to Article 9 of the Greek law on data protection that had been mentioned, to transfer of personal data to third (non-EU) countries presupposes a prior permit by the Data Protection Authority, the relevant permit was issued to Olympic Airways concerning the transfer of PNR data to Security Bureau of **Customs and Border Protection** (**CBP**) of the USA under the conditions of the relevant Agreement between the EU and USA and the European Council's decision, after prior written information of the passengers according to the relevant opinion of Article 29 Working Party.

c) SYSTEM OF PROTECTION

Furthermore, in page 32 of the paper you can see the function of this system, his technical parts with more specific details by a complete end representing analysis.

IV. CONCLUSIONS

1) The European Commission exemption clause Article 25 Section 6

Article 25 Section 6 of the Directive opens up the strict regime of the Directive for decisions given by the EC Commission stating that a specific third country ensures an adequate level of protection. In this case, Greece had to take all the measures necessary to comply with the Commission's decision. According to Article 25 Section 2, the adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer. Although Section 2 gives further instructions for this consideration, the final decision allows a broad discretion to the Commission.

Thus, the EC Commission pursues to declare the requested access of the US Customs with the given promises of data protection as consistent with the adequate level clause of Article 25. Still, this way would be very disputable for of the following reasons:

1. The Directive mainly applies to the collection of data among individuals and companies or among companies and themselves, but not among law enforcement agencies (see Article 3 "Scope" of the Directive which stipulates that the Directive shall not apply to the processing of personal data in any case to processing operations concerning public security, defense, State security). Therefore, in general, Article 25, which contains the assurance that personal data transferred to companies located in other countries meet the same level of data protection as within the EU, does not apply to data sharing between public law enforcement agencies and individuals or companies. The requested access is therefore not a matter of the regulation of data flow among companies for which the EU is solely competent for. It is a matter of cooperation with foreign law enforcement agencies which mainly still remains in the sole competence of the European Member States. As an illustration, one

could have a closer look at what airlines have to do in order to fulfill the US Customs' request. They are transferring data not for their own contractual purpose but solely at US government's request. The US could ask every passenger for the same data on their own. Instead of this, the US Customs force private companies to do so. Therefore it does not appear an exaggeration to conceive the airline companies as agencies of the US Customs. Greece was one of these countries like this example.

2. But, even if Art 25 Section 6 would in general apply, access to data for US Customs would still violate the principles of the "limitation of the purpose" as it is set forth in Article 6 (see above) of the Directive. The airlines did not originally collect data with the purpose of transferring them to US Customs and there is no specific freely given consent by passengers.

2) The opinion of the European Court.

The Court examined, first of all, whether the Commission could validly adopt the decision on adequacy on the basis of Directive 95/46/EC. It noted that Article 3(2) of the directive excludes from the directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law and, under any circumstances, processing operations concerning public security, defense, State security and the activities of the State in areas of criminal law.

According to the decision on adequacy, the requirements for the transfer of data are based on United States legislation concerning, amongst other matters, the enhancement of security, the Community is fully committed to supporting the United States in the fight against terrorism and PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes, and other serious crimes, including organised crime. Therefore, the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law. While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. That decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security

and for law-enforcement purposes.

The fact that the PNR data have been collected by private operators for commercial purposes and it is they who arrange for transfer of the data to a non-member State does not prevent that transfer from being regarded as data processing that is excluded from the directive's scope. The transfer falls within a framework established by the public authorities that relates to public security.

The Court thus concluded that the decision on adequacy does not fall within the scope of the directive because it concerns processing of personal data that is excluded from the scope of the directive. Consequently, the Court annulled the decision on adequacy. The Court added that it was no longer necessary to consider the other pleas relied upon by the Parliament.

3) National legal and political parameters.

As the European Court annuls the transfer of the PNR because of the character of this agreement has no serve commercial finalities but reason of national security and national defense that is excluded from the scope of the named directive, the Member States are in charge to judge if this is necessary or not this could take place. Although, the European Union has also renounce terrorism and is solitaire to the USA's international campaign against terrorism by the Decision of 2001 in Laaken, the Member States are exclusively responsible for sensitive personal data treatment. Ruling that the wrong legal basis was chosen since the processing operations concern public security and activities of criminal law, the Court states that it is not decisive that the data had originally been collected for commercial purposes by private agencies (the air transport of the passengers).

So, the PNR agreement must be analyzed in the frame of the treatment in general, of the personal civil data by a national state according to his legal tradition. Greek authorities must judge if the transfer of these personal data in airier travels can serve the national interest of public security, defense, State security and the activities of the State in areas of criminal law. Not the EU. So this agreement in substance was invalid.

The organization of the Olympic Games was a strong argument on this direction. But, however, with this agreement, profoundly, the biggest issue was to definite the limits between of the exercise by the national public order of the right to control by itself the treatment in the matter of the personal data or to transfer a part of this right to a third country. The balance between of these two aspects would have ensured by clear and precise items that should

enforce the legitimacy and effectivity of this operation. Thus, the reason of the insurance of the national safety as more important fact than the protection of private liberties and the rights of the personal privacy establish a very important debate on this matter for the finalities and the conditions that must be taken over.

Although, resents political evolutions in Greece show that the matter of the protection of private's rights, not only PNR but in general, is in a real danger. A track of bizarre facts that occupy the political seasonality make in worry the public opinion. Facts like the kidnap of 28 immigrants from Pakistan by British agents of the Secret Agency secretly without the permission of the Greek government in December 2005 or flights by planes of the CIA in and out of the Greek state dominion also without official permission during 2004-2007 are considered very suspicious. In particular, in February 2006 all the Greek government including Prime Minister has been spied by wiretap on their mobile phones from antennas that where have been raised in the American Embassy in Athens.

All these facts related or not with such type of agreements that concern the transfer of insensitive personal data to the USA or another third country in such a fragile historical period marked by the war against terrorism establish a sentimental of fear and insecure to Greek citizens that in January 2007 by a gallop of a well known Greek newspaper named ''KATHIMERINI'' the 61% shows to be positive to the establishment of virtual cameras policy on public space like that it was during the Olympic games. These facts are very worrying and the reasons of these effects must be inquired in the host of the Olympic games in Athens in august 2004.