9th Annual Seminar on the European Union constitutionalism
10-12 May 2010

Passenger Name Records: the transatlantic dimension

by

Katarzyna Kopyłowska
The Faculty of Law and Administration
University of Warsaw

Frauke Kruse
The Faculty of Law
Freie Universität Berlin

1. Introduction

In many respects, the terrorist attacks of 11 September 2001 mark a turning point. These tragic events, characterised by a degree of cruelty never known before, sparked off broad-based governmental measures confronting terrorism as a diffuse phenomenon of international dimensions.[1] With respect to data collected by air carriers, the terrorist attacks happened to be the crucial factor bringing about the definitive impetus for storing data of air passengers in order to combat terrorism as well as transnational crime. This policy has especially been pursued on the part of the United States.[2] Conscious of the global interrelations of air passengers' data collection as an instrument in the fight against terrorism, this article focuses on the data transfer from the European Union to the United States.

Though transfer of data collected by air carriers to the United States took place on a voluntary basis even before the terrorist attacks,[3] the Aviation and Transportation Security Act adopted on 19 November 2001 has changed quantity and quality of the transatlantic flow of air passengers' data completely. Pursuant to the Aviation and Transportation Security Act, airlines operating passenger flights within the territory of the United States are required to provide certain passengers' data to the United States.[4] In particular, the electronic access to two categories of personal data is required: on the one hand official data resulting from passports stored on air carriers' databases that shall be accessible to US authorities by means of the Advanced Passenger Information System ('APIS'), and on the other hand Passenger Name Records ('PNR'), i.e. data records created by the airlines' reservation and departure control system for every passenger – originally just for commercial purposes – containing a set of any personal data that is connected with the flight: identification data, details of reservation, travel agency, information appearing on the ticket, financial data (credit card number, expiry date, billing address, etc.), itinerary, air carrier information, seat number, and earlier PNR (e.g. details of past journeys, religious or ethnic data referring to the choice of meal, affiliation to a particular group, residence data, contact information, such as email address, address of a friend, workplace, etc., and medical data referring to medical assistance required on board), among other things.[5]

The question is whether the access of the United States' authorities to such an enormous amount of personal data of at least 10 to 11 million passengers per annum[6] by the aforementioned data transfer can be deemed necessary in order to prevent and combat acts of terrorism effectively. Taking up the European perspective, the compliance with the European law on the protection of personal data[7] and with fundamental rights and freedoms of the individual as guaranteed by the European Convention of Human Rights and Fundamental Freedoms ('the ECHR') and by the Charter of Fundamental Rights of the European Union poses serious problems.

In response to these requests for access to API and PNR data raised by the US legislation, the European Community strove for a common EU approach. Subsequently, three agreements between the European Community and the European Union respectively and the United States were concluded in order to regulate the processing and transfer of PNR data by air carriers to the United States. The first agreement of 2004 was terminated in 2006 by the European Community

---

1 See in particular the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 26 October 2001, Public Law No. 107-56.

2 See the Aviation and Transportation Security Act, 19 November 2001, Public Law No. 107-71 and the Enhanced Border Security and Visa Entry Reform Act of 2002, 14 May 2002, Public Law No. 107-173.

3 See Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, 24 October 2002, p. 2.

4 Aviation and Transportation Security Act, supra note 2, Sec. 115; Enhanced Border Security and Visa Entry Reform Act of 2002, supra note 2, Sec. 402.

5 See European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights, 13 March 2003, PS_TA(2003)0097, footnote 5; Article 29 Data Protection Working Party, Opinion 6/2002, supra note 3, p. 3.

6 See European Parliament resolution, supra note 5, preamble A.; Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, WP 78, 13 June 2003, p. 4.

7 Directive 95/46/EC, O.J. L 281/31.

as a result of a judgement from the European Court of Justice. The ensuing interim agreement concluded in 2006 was replaced by the follow-up agreement that has been in force since 2007.

Nevertheless, against the backdrop of fundamental rights and data protection the instrument of air passengers' data collection and data processing assumes still proportions which require a precise and profound analysis of the situation and reflection on the development, as particularly done by the Article 29 Data Protection Working Party.[8] Even though the transfer of PNR to the United States seems to be of declining interest since the 2007 PNR Agreement seems to regulate the matter definitively and the latest developments on this field in Europe, i.e. the approach on recording PNR inside the European Union,[9] have become the focus of attention the permanent flow of personal data to the United States must not fall into oblivion, in particular in view of the fact that the current agreement will expire in 2014,[10] and in the light of Article 218(6)(a) of the Treaty on the Functioning of the European Union which prompted the Commission to recommend to the Council the adoption of a new decision concluding the Agreement on PNR after obtaining the consent of the European Parliament.[11]

Therefore, the legal analysis of the transfer of PNR from the European Union to the United States is object of the following exposition. By describing the initial legal situation as created by the US legislation, the following EU-US Agreement on PNR of 2004 and the relating judgement from the European Court of Justice, the way shall be paved for reflections on the current legal situation on the basis of the EU-US Agreement on PNR in force.

2. The initial situation as created by the US legislation

2.1 The US legal framework

In the aftermath of the terrorist attacks of 2001, the United States created a legislation that confronted airlines operating passenger in foreign air transportation to or from the United States with an obligation to provide a passenger and crew manifest. Pursuant to the Aviation and Transportation Security Act and related implementing regulations, the passenger manifest must contain information about the passengers and crew members (name, date of birth, citizenship, passport number, country of issuance, US visa number, resident alien card number [if applicable] and such other information that is reasonably necessary to ensure aviation security) as well as PNR information upon request. This data must be electronically transmitted to the US customs authorities which is in particular the Bureau of Customs and Border Protection ('CBP', formerly the US Customs Service) as a component of the Department of Homeland Security ('DHS').[12] According to the Enhanced Border Security and Visa Entry Reform Act of 2002, air carriers were also required to provide a similar amount of personal data of passengers and crew members to the US Immigration and Naturalization Service.[13] Failure to fulfil these requirements resulted in the loss of landing

[8] See the documents of the Working Party set up by Articles 29 and 30 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, online available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

[9] European Commission, Proposal for a Council framework decision on the use of Passenger Name Record (PNR)for law enforcement purposes, SEC(2007) 1422, SEC(2007) 1453.

[10] See paragraph 9 of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), O.J. 2007 L 204/18 ff.

[11] European Commission, Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Records (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR agreement), 17.12.2009, COM(2009)702 final.

[12] See the Aviation and Transportation Security Act, 19 November 2001, Public Law No. 107-71, Sec. 115.; Passenger and Crew Manifest Required for Passenger Flights in Foreign Air Transportation to the United States, Federal Register, 31 December 2001; Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, Federal Register, 25 June 2002.

[13] See the Enhanced Border Security and Visa Entry Reform Act of 2002, 14 May 2002, Public Law No. 107-173, Sec.402.

rights and the payment of fines up to $ 5000 per error. Once transmitted to the US authorities, the data was to be stored on the Interagency Border Inspection System ('IBIS'), and therefore at the disposal of the US authorities for the lack of special provisions restricting data processing in order to protect data subjects.[14] Additionally, projects concerning mass data processing systems were developed, such as the Computer Assisted Passenger Pre-screening System II ('CAPPS II')[15] pursued by the Transportation Security Administration ('TSA'), a US authority established within the Department of Transportation by the Aviation and Transportation Security Act and later transferred to the Department of Homeland Security.[16]

2.2 The European law on data protection

Although the US legislation was addressed to air carriers it was for the European states as well as for the European Union and the European Community to deal with this matter owing to the European law on data protection. For personal data meaning any information relating to an identified or identifiable individual,[17] the collection of PNR data as personal data falls clearly within the scope of data protection law. With respect of Article 8 of the ECHR as interpreted by the European Court of Human Rights and of the Convention No. 108[18] by which the member states of the Council of Europe are bound, and which was respected by the European Union at that time by means of Article 6 (2) of the EU Treaty (version of Masstricht), and with respect of Article 7 and especially Article 8 of the Charter of fundamental rights of the European Union respected by the European Union at that time by means of Article 6 (2) of the EU Treaty (version of Maastricht), the individual's right to privacy in its particular shape of protection of personal data is set down. Furthermore the Community Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the related legislation of the member states has developed legal safeguards to protect data subjects referring to matters of the internal market. It follows from this that the responsibility of the member states and the European Union to safeguard the individual's right to privacy.

2.3 The conflict of US and EU law

The compliance of the US legislation, demanding for an extensive collection of PNR data including sensitive data as defined in Article 8 of Directive 95/46/EC, uncontrollable by the data subject, with the right to privacy as granted by aforementioned provisions was assessed to be eminently questionable by the Article 29 Data Protection Working Party as well as by the European Parliament which expressed apprehensions that European airlines' databases would be used for "data-mining" by US authorities.[19] After the Commission informed the US authorities in June 2002 about the possible incompatibility of the US requirements with the European law on data protection with the result that the entry into force of the US provisions was postponed until 5 March 2003, negotiations between the Commission and the US administration were launched in order to reconcile the requirements by entering into an international agreement.[20] As a result, the first PNR

---

14 The right to data protection refers only to US citizens and aliens lawfully admitted for permanent residence, 5 United States Code, Sec. 552a (a) (2).

15 See Privacy Act of 1974: System of Records, Federal Register, 1 August 2003.

16 See also Article 29 Data Protection Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, 24 October 2002, pp. 3 f.; Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, WP 78, 13 June 2003, p. 5.

17 See Article 2 (a) of Convention No. 108 (infra note 18) and Article 2 (a) of Directive 95/46/EC.

18 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series, No. 108, 28 January 1981, entered into force on 1 October 1985.

19 European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights, 13 March 2003, PS_TA(2003)0097, in particular preamble C.; Article 29 Data Protection Working Party, Opinion 6/2002, supra note 16.

20 See European Commission/US Customs Talks on PNR Transmission, Joint Statement, 17/18 February 2003; Commission of the European Communities, Communication from the Commission to the Council and the

EC-USA Agreement came into force on 28 May 2004.[21] In the meanwhile, between 5 March 2003 and 28 May 2004, European airlines were under pressure to fulfil the US requirements whilst getting thereby under control of the European data protection authorities. Several European airlines facing the US sanctions fulfilled the requirements and provided access to PNR data.

3. The 2004 PNR EC-US Agreement

The basis for the first Agreement on PNR was constituted by two corresponding documents: on the part of the European Union a Decision on Adequacy adopted by the Commission,[22] on the part of the United States an Undertaking of CBP.[23]

Applying Directive 95/46/EC, the Commission is entitled, pursuant to Article 25 (6) thereof, to decide whether a third country ensures an adequate level of protection since the member states must provide an adequate level of protection pursuant to Article 25 (1) whenever data transfer to a third country for processing purposes takes place. Therefore, in the case of data transfer from a member state to a third country, in the present case to the United States, the adequate level of protection required is ensured by the adequacy decision of the Commission that dispenses the member state from giving additional guarantees,[24] and facilitating thereby the data transfer considerably. In particular, the Decision adopted by the Commission certificates the adequacy of the level of protection for PNR data transferred from the Community concerning flights to or from the United States ensured by CBP as far as CBP abides by its Undertaking on the processing of PNR data. Thereby, the member states' power to suspend data flows to the United States as a third country is reduced to cases enumerated in Article 3 of the Commission's Decision 2004/535/EC concerning deviations from the Undertaking.

The Undertaking itself was supposed to define the conditions of the PNR data processing by CBP, and thereby forming the basis for the adequacy finding of the Commission. Only this document contains the substantial statements concerning the concrete technical questions about PNR data.

The Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection[25] determines the electronic access of CBP to the European air carriers' reservation/departure control system and places an obligation on the European air carriers to process PNR data as required by CBP on certain conditions (paragraph 1 and 2). As for the level of commitment of the Decision on Adequacy and the Undertaking, CBP "takes note" of the Decision of Adequacy and "states" the implementation of the Undertakings.

On behalf of the European Community, the Council approved the Agreement by adopting Decision 2004/496/EC.[26] Considering the matter of transfer of PNR data by European airlines to the CBP to be an external aspect of the establishment and functioning of the internal market that required harmonisation of the conditions of competitions between the member states'

Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, 16 December 2003, COM(2003) 826 final.

21 See the Information of the Council concerning the entry into force of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, O.J. 2004 C 158/1.

22 Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection (2004/535/EC), O.J. 2004 L 253/11.

23 Undertaking of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), published as annex to the Commission Decision 2004/535/EC (supra note 22) in O.J. 2004 L 253/15.

24 See second recital in the preamble of the Commission Decision 2004/535/EC, supra note 22.

25 O.J. 2004 L 183/84 (referring to an incorrect reference for the Decision of Adequacy subject of corrigendum, O.J. 2005 L 255/168).

26 Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC), O.J. 2004 L 183/83.

airlines, the Council Decision was based on Article 95 EC Treaty, in conjunction with the first sentence of the first subparagraph of Article 300 (2) EC Treaty.

4. The assessment of the 2004 PNR EC-US Agreement

This legal framework consisting, from the European point of view, of the international Agreement, the Decision on Adequacy, the Undertaking of CBP and the Council Decision was subject of severe criticism, passed on by the Article 29 Data Protection Working Party[27] and by the European Parliament,[28] as well as by the legal literature[29] and by non-governmental organisations.[30] Without elaborating the reservations concerning the compliance of the 2004 PNR Agreement with the European law on data protection for substantially similar questions will be subject of a particular analysis referring to the current Agreement on PNR the major areas of concern are, nevertheless, described in outline.

In particular, the purpose for which PNR data was used by CBP was considered to be too broad, since the use of PNR data involved "purposes of preventing and combating: 1. terrorism and related crimes; 2. other serious [transnational] crimes […]; and 3. flights from warrants or custody for [these crimes]" (paragraph 3). As for the scope of PNR data to be collected, the list including 34 fields of personal data[31] was deemed unnecessarily wide, and the data retention period of a minimum of three and a half years (paragraph 15) was assessed as excessive as well. With respect to CAPPS II, CBP reserved the right to transfer PNR into this system for testing purposes (paragraph 8), against the explicit advice given by the Article 29 Data Protection Working Party. Another point of critique was the method of accessing PNR data according to which CBP was allowed to "pull" PNR from air carriers' databases until a system was implemented enabling air carriers to "push" the required PNR data to CBP (paragraphs 12-14). In addition, the transfer of PNR data to other governmental or foreign authorities raised questions since the potential recipient authorities as well as the conditions for such a transfer were not clarified (paragraphs 29, 34, 35). In general, the validity of statements which aimed at the assurance of a certain level of data protection was weakened by exceptions, inaccurateness of terms and discretionary powers of CBP. Furthermore, the level of commitment was considered to be questionably low, in particular for the fact that the Undertaking was given by CBP as component of the administration, that the level of data protection assured was not based on legislative acts and that the Undertaking integrated

---

27 See Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, WP 78, 13 June 2003; Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), WP 87, 29 January 2004; Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, WP 95, 22 June 2004.

28 See European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, 31 March 2004, 2004/2011(INI); Applications of the European Parliament in the cases C-317/04 and C-318/04, O.J. 2004 C 228/31 f.

29 See for instance Maarten Peeters, *Security Policy vs. Data Protection – Transfer of Passengers' Data to U.S. Authorities*, MultiMedia und Recht 2005, pp. 11-17.

30 See for instance Privacy International, Inadequate Adequacy, May 2004.

31 PNR data elements required pursuant to Attachment A: PNR record locator code, date of reservation, date(s) of intended travel, name, other names on PNR, address, all forms of payment information, billing address, contact telephone numbers, all travel itinerary for specific PNR, frequent flyer information (limited to miles flown and address(es)), travel agency, travel agent, code share PNR information, travel states of passenger, split/divided PNR information, e-mail address, ticketing field information, general remarks, ticket number, seat number, date of ticket issuance, no show history, bag tag numbers, go show history, OSI information, SSI/SSR information, received from information, all historical changes to the PNR, number of travellers on PNR, seat information, one-way tickets, any collected APIS information, ATFQ (Automatic Ticketing Fare Quote) fields. Pursuant to paragraph 7, this list was extensible in order to fulfil the purposes of paragraph 3.

unilateral amendments on the part of the United States. These legal concerns proved to be justified in the light of the joint review of the implementation of the Undertaking.[32] In spite of the general finding of a substantial compliance with the Undertaking, the single undertakings turned out to be implemented not before May 2005, and thus about one year after the Agreement was concluded. From a data protection point of view, the 2004 PNR Agreement was for these reasons generally assessed as an encroachment of the passengers' right to privacy.

5. The European Court of Justice judgement on the 2004 PNR EC-US Agreement

Owing to the substantial reservations about the Council Decision 2004/496/EC and the Decision 2004/535/EC on Adequacy, the European Parliament, supported by the European Data Protection Supervisor, brought an action against the Council of the European Union and an additional action against the Commission of the European Communities for annulment under Article 230 EC Treaty before the Court of Justice of the European Communities ('the ECJ'), both on 27 July 2004. The cases C-317/04 and C-318/04 were subsequently joined. As proposed by the Advocate General,[33] the Court in the form of the Grand Chamber annulled the Council Decision as well as the Decision on Adequacy.[34]

As for the Decision on Adequacy based on Article 25 (6) of the Directive 95/46/EC, the Court found that this decision was not covered by the scope of the Directive as defined in Article 3 thereof. Pursuant to the first indent of Article 3 (2) of the Directive, "the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the States in areas of criminal law" is excluded from the scope. Aware of the fact that the collection of PNR data by air carriers initially took place in connection with a supply of services and thereby within the scope of Community law, the Court held that the data processing in question was deemed necessary for "safeguarding public security and law-enforcement purposes". Accordingly, the Decision on Adequacy concerned processing operations as defined in the first indent of Article 3 (2) of the Directive. Because of the Directives' scope being infringed, the Court annulled the Decision on Adequacy.[35] As for the annulment of the Council Decision, the Court based its decision on the finding that Article 95 EC Treaty does not cover a Community competence to "conclude [an] agreement [that] relates to the same transfer of data as the decision on adequacy and therefore to data processing which […] are excluded from the scope of the Directive".[36] Since the termination of the Agreement between the European Community and the United States, pursuant to paragraph 7 thereof, took 90 days from the date of notification of termination to the other party the Court limited the effect of the annulment in regard to the Decision on Adequacy, inasmuch as it preserved the effect of this decision until 30 September 2006 in order to guarantee legal certainty.[37]

Despite the fact that the result of the judgement had been expected in the light of the massive doubts about the legitimacy of the decisions, the line of reasoning, namely that the Court reduced the matter to a question of competence and abstained from any remark on the substantial problematic of data protection, raised questions. Not only left the Court the question about the sound legal basis of the council decision unresolved,[38] but also failed the Court to point out the

---

32 See Commission Staff Working Paper on the Joint Review of the implementation by the U.S. bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of May 2004, redacted version, 12.12.2005, COM (2005) final.

33 See Opinion of Advocate General Léger, 22 November 2005, cases C-317/04 and C-318/04.

34 Joined cases C-317/04 and C-318/04.

35 Ibid., paragraphs 54–61.

36 Ibid., paragraphs 67–70.

37 Ibid., paragraphs 71–74.

38 The Advocate General mentions this "interesting" questions without pursuing the matter, see Opinion (supra note 33), paragraph 157.

negative effects on data protection caused by the Agreement and to establish criteria for the balance between the fight against international terrorism and the right to privacy or at least minimum requirements concerning data protection, and to pave the way for an – inevitably necessary – new agreement on PNR that would have taken data protection into account in accordance with European law.[39]

The judgement led de facto to the termination of the first Agreement on PNR between the European Community and the United States, creating thereby a legal vacuum and the urgent need for a new agreement that proves in the form of the 2007 PNR Agreement to be less effective concerning data protection than the annulled framework on PNR what will stated below. Therefore, the judgement might be rightly referred to as "a poisoned chalice for those who sought it".[40]

6. The 2006 PNR EU-US Agreement

In view of the necessity to conclude a new agreement in order to avoid a situation of legal uncertainty which would have been caused by the absence of any agreement on PNR transfer for the European passengers concerning the protection of their PNR data, and the European airlines confronted with the US sanctions alike, the European and US sides began another round of negotiations.[41] As a result, in October 2006 the European Union and the United States entered into an interim agreement[42] which was accompanied by a letter from the Department of Homeland Security specifying the Undertaking of the CBP of 2004. This agreement was replaced in 2007 by a long-term agreement on PNR that is still in force.

7. The 2007 PNR EU-US Agreement

Under the pressure to conclude a new agreement owing to the expiration of the short-term agreement on 31 July 2007 at the latest, the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)[43] was signed on 23/26 July 2007. Supplementary, the European Union and the United States exchanged letters concerning the handling of PNR data by the DHS. Whilst the US letter to EU ('DHS's letter') "explain[s]" the handling of PNR data, "provides assurances" and "reflects the policies" on PNR data the replying letter is limited to the statement that the level of data protection the US side ensures according to its letter is deemed adequate.[44] As the CBP Undertaking of 2004 is not referred to any more, the assurances of the DHS's letter establish the single basis of the Agreement by which the European Union is obligated to ensure the data transfer from the air carriers' reservation systems. On behalf of the European Union, the Agreement was approved by Council Decision 2007/551/CFSP/JHA.[45]

---

39 See Michele Nino, *The protection of personal data in the fight against terrorism, New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon*, Utrecht Law Review 1/2010, pp. 62-85 (p. 74).

40 See Gráinne Gilmore/Jorrit Rijpma, *Joined Caes C-317/04 and C-318/04, European Parliament v. Council and Commission, Judgement of the Grand Chamber of 30 May 2006, [2006] ECR I-4721*, Common Market Law Review 4/2007, pp. 1081-1099 (1099).

41 See the instructions by the Article 29 Data Protection Working Party as expressed in Opinion 2/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, WP 122, 14 June 2006 and in Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, WP 124, 27 September 2006.

42 Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, O.J. 2006 L 298/30.

43 O.J. 2007 L 204/18.

44 The text of the letters is published as annex to the Council Decision (infra note 45), O.J. 2007 L 204/ 21.

45 Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)

Compared with the 2004 PNR Agreement, a dual change took place. In formal respects, the Council Decision is based on Article 24 and 38 of the EU Treaty as a consequence of the ECJ judgement in the joined cases, and thus within the scope of the third pillar. Hence, the European Union is party to the Agreement instead of the European Community. In material respects, the level of data protection remained under the level ensured by the 2004 PNR Agreement owing to the extension of exceptions and imprecise wording.[46] The resulting legal problems concerning the compliance of the 2007 PNR Agreement with the European law on data protection are subject of legal analysis in the following.

7.1 Legal frame of data processing

The technological development and the progress of application of computer technology in data processing raised doubts, if legal protection of right to respect for privacy on the ground of Article 8 of the European Convention on Human Rights is sufficient, when referred to the automated data processing. The new threat to fundamental rights became an impulse for adopting in 1981 the Council of Europe Convention No. 108 for the protection of individuals with regard to automathic processing of personal data[47] – the purpose of the Convention was specified as „securing in the territory of each Party, for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particulary his right to privacy, with regard to automatic processing of personal data relating to him". Bearing in mind the doubts relating the scope of protection on the basis of Article 8 of the European Convention on Human Rights, the European Union guaranteed in Article 8 of the Charter of Fundamental Rights of the European Union[48] the right to the protection of personal data, regardless of the right to respect for private and family life. The national legislation concerning the protection of individuals with regard to personal data processing followed the principles of protection that were constituted in the Convention.

Alongside with the formation of common market the Council and the Parliament of the European Union perceived the pressing need for the harmonization of the regulations on protection of personal data as the differences in the level of protection in the Member States could prevent the transmission of such data between the Member States and become an obstacle to development of four freedoms. On 24 October 1995 the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[49] was adopted. The Directive's purpose was to balance the high level of protection of right to privacy of the individuals and the public interest in processing of personal data.[50] The Directive 95/46/EC in comparison to the Convention No. 108 is characterized by the highly detailed regulations – the Directive of the European Union claryfies and developes the provisions from the Convention. Both Convention and the Directive do not apply within the scope of the third pillar, to which the Agreement between the European Community and the United States of America on the processing and transfer of PNR data belongs.

The standards for the protection of rights of data subject and data processing in third pillar are set in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[51] Most of the provisions in Council Framework Decision 2008/977/JHA mirror the other EU legal instruments on the protection of personal data, but also provide additional set of

(2007 PNR Agreement), O.J. 2007 L 204/ 16.

46 See Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, 17 August 2007.

47 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series, No. 108, 28 January 1981, entered into force on 1 October 1985.

48 Charter of the Fundamental Rights of the European Union, O.J. C 364/1

49 O.J. L 281/31.

50 Arwid Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, Państwo i Prawo 06/1997.

51 O.J. L 350/60.

rules taking into account the specific nature of the area of law enforcement.[52] Nevertheless the principles of data protection in Council Framework Decision are not in line with the principles of the Directive 95/46/EC, which set the highest level of protection. The European Data Protection Supervisor in his third opinion[53] expressed criticism of inconsistency of the provisions of the Framework Decision with the protection level guaranteed by the Directive 95/46/EC and Convention No. 108 – in his opinion „[the Framework Decision] fails to provide the added value to Convention 108 which would make its provisions appropriate from a data protection point of view, as required by Article 30(1) of the EU-Treaty. Secondly, it also fails to meet in many aspects the level of protection required by Convention No. 108." European Data Protection Supervisor also emphasized that Framework Decision do not ensure an adequate level of protection for exchanges with third countries[54], which is crucial considering the PNR data transmission to the U.S. agencies.

On the basis of abovementioned legal acts, the PNR processing should fill the following condition:

- processing of PNR data should be fair and lawfull
- processing should serve specified, explicit and legitimate purposes without further processing in a way incompatible with those purposes
- personal data must be accurate and kept up-to-date
- personal data must be kept in a form which permits identification of data subject for no longer than is neccesary for the purpose they were collected (data retention period)
- processing should be adequate, relevant and not excessive in relation to the purpose for which data are collected or futher processed
- the third country, to which the data are transferred, must ensure an adequate level of data protection

The aim of the following part of the essay would be to examine in the detailed manner the provisions of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data according to the aforementioned principles.

7.2 The scope and the legal classification of the Agreement

For a contextualised examination of single provisions of the 2007 PNR Agreement concerning the use of PNR, and for a profound analysis of their compliance with European data protection law, general consideration should be given to those issues applying to all provisions in the same way; that is, on the one hand, the scope of passengers affected. Pursuant to paragraph 1 of the 2007 PNR Agreement, PNR transfer from those air carriers "operating passenger flights […] to or from the United States" is required, but it remains unclear which kind of relation between the EU and the airline leads to the obligation to transmit PNR to DHS. Taking the broadest interpretation as a basis, even PNR from databases of airlines who operate from outside of the EU a transit through the EU could fall within the scope of the Agreement.[55] Hence, the scope of passengers affected by the PNR data collection and processing by DHS is not unambiguously defined.

On the other hand, the level of commitment of the Agreement and especially of DHS's

---

[52] Second opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2007/C 91/02, O.J. C 91/9.

[53] Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2007/C 139/01, O.J. C 139/1.

[54] *EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step*, press release of European Data Protection Supervisor, Brussels Friday 28 November 2008.

[55] See Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, 17 August 2007, p. 7.

letter raises questions. The Agreement itself is binding upon the parties, though the United States are merely represented by DHS as part of the administration. DHS's letter, however, and thereby the part which contains the most substantial provisions concerning the data protection standard offered by DHS does not "create or confer any right or benefit on any person or party, private or public, nor any remedy other than that specified in [the Agreement]", just as the Undertaking of CBP of 2004.[56] But in contrast to the latter by which CBP "undertook" to handle PNR data as laid down, the letter, merely, "provides assurances and reflects [DHS's] policies [on PNR]" according to its preamble. Thus, the level of commitment remains under the low binding level of the Undertaking. The single instrument of the European Union to control the implementation of the provisions of DHS's letter is the review as described in paragraph 4 of the 2007 PNR Agreement and in paragraph X of DHS's letter. The review system, however, has been weakened as well. Whilst the Undertaking ensured an annual review assisted by European law enforcement authorities and/or authorities of the member states[57] the DHS's letter provides only for a periodical review, and does not require any independent assistance during the review process. In fact, the first review of the implementation of the 2007 PNR Agreement took place on 8/9 February 2010; almost three years after the Agreement came into force, and on behalf of the European Union merely represented by a delegate of the Commissioner for Justice, Freedom and Security.[58] The conclusion of the joint review finds the Agreement for the most part appropriately implemented by DHS, but as pointed out by the Article 29 Data Protection Working Party,[59] the fact that both parties have to agree mutually on the review might lead to disregard of controversial issues.

Taking into account the inaccuracy of the scope and the low level of commitment of the 2007 PNR Agreement, the compliance of single provisions with the aforementioned principles of European data protection law is analysed in the following.

7.3 The purpose limitation principle

The purpose limitation principle, involving the consideration that any data collection requires a clear objective to be achieved in order to restrict data collection and processing effectively, determines that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[60]

The purpose of PNR data collection by DHS is basically defined as preventing and combating terrorism and transnational crime, pursuant to the first recital of the preamble of the 2007 PNR Agreement. This is specified in paragraph I of DHS's letter which describes "preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above" as purposes, and is almost literally identical to the purposes laid down in the former agreements on PNR. Likewise with the previous agreements, the lack of definition is contrary to the purpose limitation principle. As long as the meaning of terrorism-"related crimes" and "other serious crimes" is not defined at all the purpose limitation remains precariously broad, and conditional upon DHS's interpretation. Additionally, DHS's letter contains new purposes for the use of PNR data, namely "where necessary for the protection of the vital interest of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law". Compared with the Undertaking of CBP in 2004 which mentioned those issues in the context of onward transfer,[61] the

---

56 See supra note 23, paragraph 47.

57 See supra note 23, paragraph 43.

58 Commission, Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), 8-9 February 2010, Brussles on 7.4.2010.

59 See Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, 17 August 2007, p. 14.

60 See Article 5 (b) of Convention No. 108; 28th recital in the preamble and Article 6 (b) of Directive 95/46/EC.

61 See paragraph 34 and 35 of the CBP Undertaking (supra note 23);

classification as purpose rather than as possible use displays the intention to broaden the limitations of purpose. The added purposes raise further questions in substantial respects. As for the use on behalf of vital interests, the possible scenario of those cases is left open.[62] As for the use in "any" criminal proceeding, it implies that PNR data collection aims at the use of those data even for petty crimes and offences far away from terrorism.[63] As for the use "as otherwise required by law", this clause makes a unilateral extension of purposes possible.

It follows from this that the purposes laid down in DHS's letter are definitely too broad formulated. Aware of the elusiveness of crimes relating to international terrorism as a diffuse phenomenon, data protection law requires a certain degree of purpose limitation on behalf of the millions of unsuspicious passengers deeply affected by the PNR data collection. The purposes in question, however, are too vague defined to offer certainty about the dimensions of PNR data collection. Therefore, the purposes as given in DHS's letter are, admittedly, legitimate in principle, but by no means explicit and specified. Hence, the purpose limitation principle is infringed.

As a result of the lack of a sound purpose limitation, this problem emerges in almost every matter about how to handle PNR data again for the fact that deviations from data protection standards are justified by reference to the purposes.

7.4 The processing of PNR data

European data protection law stipulates that personal data must be fairly and lawfully processed.[64] In this context, processing means any operation or set of operations which is performed upon personal data.[65] Taking this meaning as a basis, PNR data is subject of processing in a large variety of different ways. An agreement on PNR transfer which aims to fulfil European data protection standards must therefore provide for the fairness and lawfulness of the processing of PNR data transferred in the course of the implementation of the agreement. Whether the current Agreement reaches those standards is profoundly questionable for the premises laid down turn out to be unspecific, and even more unilaterally modifiable.

According to paragraph 3 of the 2007 PNR Agreement, the processing of PNR data is determined by "applicable U.S. laws, constitutional requirements, and without unlawful discrimination […]" whilst fundamental rights and the protection of personal data are merely once mentioned in the preamble. Even though the US law on data protection, namely the US Privacy Act, includes now EU citizens as well it is left open which specific US legislation is applicable, and if European data protection standards are fulfilled.[66] From the European point of view, the general reference to US law does not appear to determine the processing of PNR data in an adequate way.

The manner of processing is explicitly touched in paragraph II of DHS's letter as regards sharing of PNR data. Thus, PNR data shall be shared only in accordance with the purposes for which PNR is used. Since the purposes are too broad and unspecific defined as outlined above the assurance to process PNR only for those purposes is de facto no restriction of processing. In particular, the reference to the purposes which include even crimes not related to terrorism as stated above entitles DHS to share PNR data even for investigations about non-terrorist crimes. In the absence of any list, defining which unit of DHS is entitled to be recipient of PNR data, DHS as a whole is recipient in contrast to the Undertaking of CBP of 2004. From this follows an extension of those US authorities which have access to PNR and can process PNR without fulfilling any conditions. As for the onward transfer to domestic government authorities or other government

---

62 Even the definition as given in the US letter accompanying the interim Agreement on PNR (supra note 42) is rather inaccurate: "'Vital interest' encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay."

63 See Article 29 Data Protection Working Party, Opinion 5/2007, supra note 51, p. 8.

64 See Article 5 (a) of Convention No. 108; Article 6 (a) of Directive 95/46 EC.

65 See Article 2 (b) of Directive 95/46/EC.

66 European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, P6_TA(2007)0347.

authorities in third countries, former explicit provisions on the manner of transfer, including a case-by-case-basis and a certain degree of control by CBP as the "owner" of PNR,[67] no longer apply. Instead, the eligible authorities and the transfer itself are vaguely described, and the control of shared PNR data is not mentioned at all. Accordingly, the provisions on sharing of PNR do not provide for a fair and lawful processing for the lack of any clarifying binding basis.

As a result of the analysis of the compliance with the principle of fair and lawful processing, the underlying cause of doubts regarding the fairness and lawfulness is the absence of a sound legal framework concerning the broad field of processing. In particular with regard to sensitive data, the statements to filter those PNR and not to use it except for emergency cases (paragraph III) is not sufficient considering the deep interference with the right to privacy and the European standards concerning sensitive data.[68] Taking the Agreement and DHS's letter as a basis, the dimensions of processing are unforeseeable, and therefore non-compliant with the principle of fair and lawful data processing.

7.5 The data retention period

From the European law on data protection follows as well that personal data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purpose for which those data are collected or processed.[69] In the context of the EU-US Agreements on PNR data, this matter is referred to as data retention period. The data retention period, likewise all detailed provisions on PNR data collection and processing, is subject of the DHS's letter, in particular of paragraph VII thereof.

As for the scope of data to which the retention period as prescribed by DHS's letter applies, even the data collected on the basis of the former EC/EU-US Agreements on PNR are included. Hence, PNR data, transmitted on the basis of the former agreements which referred to the Undertaking of the CBP of 2004 assuring a general storage period of three and a half years, is now subject to the new retention period. The Article 29 Data Protection Working Party assessed this procedure as an unacceptable unilateral extension of the retention period.[70]

As for the data retention itself, there is made a distinction between data retention in general, and exceptions for data related to a specific case or investigation. Principally, PNR data is retained in an active analytical data base for seven years, and thereafter in a dormant, non-operational status for eight years. The storage of data in dormant status means that access to those data depends on two additional conditions to be fulfilled; these are in particular the approval of a certain DHS officer, and relations to an identifiable case, threat, or risk. Whether PNR data after these 15 years will be deleted is left open. Regarding the deletion, the provision refers to future discussions of DHS and EU.

Analysing this concept of data retention from a data protection point of view, the difference between active and dormant storage is irrelevant to the overall duration of the data retention. Even in dormant status, the data storage permits identification of the data subject, merely on additional conditions of access. Decisive is, however, the availability of data, according to aforementioned law on data protection. Thus, the data retention period amounts to 15 years, and taking into account that the circumstances of deletion are not clarified, is perhaps even longer. In summary of the technical side of data retention, every passenger's PNR that is transmitted to DHS is kept in form which permits identification of the data subject for 15 years, at least.

The compliance of this data retention period with the standards of European data protection law depends upon whether the retention period is no longer than necessary in the light of the purpose for which the data are collected or processed. Following the case law of the European

---

67 See paragraphs 28-35 of the Undertaking of CBP (supra note 23).

68 See Article 8 of Directive 95/46/EC.

69 See Article 5 (e) of Convention No. 108; Article 6 (e) of Directive 95/46/EC.

70 Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, 17 August 2007, p. 13.

Court of Human Rights, a measure is "necessary" within the meaning of Article 8 (2) of the ECHR provided that "a pressing social need" is involved and the measure is "proportionate to the legitimate aim pursued".[71] Leaving the aforementioned problems concerning the inaccurateness of the purpose aside, the purpose of PNR data collection and processing by DHS, namely preventing and combating international terrorism, is in substance undoubtedly legitimate. A data retention period of 15 years, however, proves to be disproportionate to this aim. Even though the need for data retention in general is usually explained by the need to examine risk indicators and behavioural patterns[72] it does not appear that a long-term retention restricted to cases which are subject to investigation would be significantly less effective. The necessity to extend the data retention period from three and a half years up to 15 years is not evidenced. Additionally, the storage of PNR data in an active analytical data base for seven years might facilitate massive profiling and data mining.[73] Considering the amount of persons affected without any suspicion,[74] and considering the intensity of interference with their right to privacy by storing their PNR data for 15 years, the purpose of preventing and combating international terrorism cannot justify such a long data retention period.

It follows from this that PNR data is kept in a form which permits identification of the data subject for longer than is necessary for the purpose for which those data are collected or processed, and that the data retention period as set down in the DHS's letter is non-compliant with EU law on data protection.

7.6 The accuracy and topicality of processed PNR data

7.6.1 The principles of quality of PNR data

The Convention No. 108 for the protection of individuals with regard to authomatic processing of personal data in Chapter II creates a set of rules concerning the quality of processed personal data. Point (d) of Article 5 of the Convention No. 108[75] includes the condition of accuracy and topicality of processed and transferred personal data. The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and to the free movement of such data[76] in Article 6 establishes an additional obligation for the Member States to erase or rectify the inaccurate or incomplete data. The Council Framework Decision on the protection of personal data processed in framework of police and judicial cooperation in criminal matters[77] specifies the positive obligation of the competent authorities which are responsible for veryficating the quality of collected and transmitted personal data. Article 8 of the Council Framework Decision constitutes that „the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability". The same principles regarding the quality

---

71 European Court of Human Rights, Gillow vs. United Kingdom, judgement of 24 November 1986, Series A No. 109, paragraph 55.

72 See in the context of a European PNR system the Commission Staff Working Document, Accompanying document to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Impact Assessment, 6.11.2007, SEC(2007) 1453, p. 32.

73 European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America, P6_TA(2007)0347, paragraph 20.

74 The Acting Director of the US Visit Programme referred to 1200 criminals and immigration violators out of 63 million passengers, see House of Lords, European Union Committee, 21st Report of Session 2006-07, The EU/US Passenger Name Record (PNR) Agreement, Report with Evidence, published 5 June 2007, Oral evidence, 21 March 2007, Q89 (p. 30), online available at:
http://www.publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf.

75 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108, 28 January 1981

76 Directive 95/46/EC, O.J. 1995 L 281/31.

77 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L 350/60.

of data apply to personal data transferred to the third States. The abovementioned principles of data quality are in great importance according to the Passenger Name Record data as information sharing is an essential component in the fight against terrorism – PNR data system should serve to prevent terrorism attacks by creating profiles of unknown perpetrators and by identyfing the travel patterns of the members of terrorist organisations. Every misleading information or fact derived from inaccurate or incomplete data may entail the institution of investigation against an innocent passenger. The risk of missidentification and mistake can also be the result of erroneous interpretation of PNR data, even if they are accurate. The Agreement between the United States and the European Union and the explanatory letter of the Secretary of Homeland Security do not contain any additional provision concerning the quality of transferred PNR data – the principles of the Directive 95/46/EC, Convention No. 108 and the Council Framework Decision 2008/977/JHA will find application to the quality of PNR data.

In the light of the Agreement it is the air carriers' obligation to transmit the PNR data directly to the U.S. Department of Homeland Security – as a consequence the air carriers are responsible for ensuring the accuracy of transferred personal data. Unlike API data, some of the types of the collected PNR record are provided by passenger on voluntary basis – the accuracy of such data can not be checked by air carriers, because they are not entitled to verify the received PNR data. The Association of European Airlines rightfully underlined, that due to lack of proper measures to verify the PNR data air carriers shouldn't be held liable for transmitting incorrect or incomplete records.[78] Since there is no subject responsible for controlling the accuracy of PNR data, the reliability of transmitted information and the value of PNR data in assessing risk becomes questionable.[79]

7.6.2 Rights of the PNR data subject

1. Right to information on personal data processing

Article 8 of the Charter of Fundamental Rights of the European Union proclaims the positive obligation of obtaining prior consent of individual to whom the personal data refer as a condition of lawful personal data processing. Consent can only be considered valid if the individual has the necessary information concerning inter alia the scope of processed personal information, the subject authorisied to processing the data, the level of protection ensured by this subject, the data retention period and his right to access the personal data. According to the transparency principle on the basis of Directive 95/46/EC (Article 10-11) and Convention No. 108 (Article 8) , the passengers whose PNR data will be processed, should receive a complete, accurate and timely information before purchaising the ticket, not only in cases where their consent is necessary, but in every situation of personal data processing.

Neither the Agreement, nor the letter of the Secretary of Homeland Security do not stipulate *expressis verbis* the passenger's right to information – point (7) of the Agreement includes only vague provision, that "the U.S. and the EU will work with interested parties in the aviation industry to promote greater visibility for notices describing PNR systems (including redress and collection practices) to the travelling public and will encourage airlines to reference and incorporate these notices in the official contract of carriage". Furthermore the Department of Homeland Security commits itself to "provide to airlines a form of notice concerning PNR collection and redress practices to be available for public display". None of the abovementioned acts indicates who shall be responsible for informing passengers on processing of their PNR data – it is to be assumed, that the Agreement burdens the air carriers and travel agents with the obligation of informing

---

[78] Evelien Brouwer, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?*, Center for European Policy Studies Working Document No. 320 (September 2009).

[79] Joint opinion of the Article 29 Working Party on the proposal for a Council Framework Decision on the use of PNR for law enforcement purposes adopted on 5 December 2007.

passengers on processing of the PNR data.

The significance of the transparency principle was repeatedly emphasised in the opinions of Article 29 Working Party.[80] The Article 29 Working Party in the annex 1-3 to the opinion 2/2007[81] has adopted the information notices that should serve as a guidance on PNR processing for passengers on transatlantic flights with the recommendation to use the following information notices as broadly as possible by air carriers, travel agents and computer reservation systems.

2. Right to access to the personal data and rectification

The individual's right to access to his personal data and the right to rectification of incorrect personal data complements the right to information. Nevertheless according to Article 13 of the Directive 95/46/EC and Article 17 of the Council Framework Decision the right to access might be restricted by legislative measures adopted in the Member States to inter alia safeguard public or national security or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences.

The provisions in the letter of Secretary of Homeland Security ensure the passenger's right to access and rectification of PNR data. The Secretary in his letter assures that "PNR furnished by or on behalf of an individual shall be disclosed to the individual in accordance with the U.S. Privacy Act and the U.S. Freedom of Information Act (FOIA). FOIA permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA", including the PNR data that relates the European Union citizens. This commitment met the approval of the Article 29 Working Party[82], who pointed out in previous opinion adopted on 13th June 2004[83] the possible threat of discrimination between U.S. citizens and non-U.S. citizens in enforcing their right to access and rectification. Furthermore the Article 29 Working Party underlined that the right to access should extend to any information generated in PNR data processing, not PNR data only.

Despite the fact that the denial or postpone disclosure of PNR record can be administratively or judicially challenged, it is to state that in practice the enforcing of individual's right to access and rectification before the court might be difficult for the European Union passengers, because of the ignorance of United States law as well as because of the practical obstacles.

In conclusion it is to be scrutunized that the procedural safeguards of individuals' right to personal data access and rectification are not precisely constituted in the act of Agreement. Furthermore the right to rectification is not the part of the Agreement itself, but is contained in accomplying letter of the Secretary of Homeland Security. The letter in Article IV concerning the enforcement measures available to passengers refers to policies on the DHS website. That form of ensuring individual's right is inadmissible.

---

80 See for example: The Article 29 Working Party, opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection adopted on 29 January 2004; The Article 29 Working Party, opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007.

81 The Article 29 Working Party, opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities adopted on 15 February 2007 and revised and updated on 24 June 2008; See also: The Article 29 Working Party, opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America adopted on 30th September 2004.

82 The Aricle 29 Working Party, opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007.

83 The Article 29 Working Party, opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data adopted on 13 June 2004.

3. Voluntariness of passenger's consent

According to the Article 8 of the Charter of Fundamental Rights processing of personal data must be preceded with consent of the data subject whose personal data are to be processed. Article 2(h) the data subject's consent is defined as "freely given specific and informed indication of his wishes". Bearing in mind the consequences of denial of such consent by the transatlantic passenger, the voluntariness of consent to processing and transferring of PNR data is called in question – such denial would inevitably lead the passenger to not being able to board the plane.[84]

7.7 Principle of proportionality and neccesity

In the preamble of the Agreement on the processing and transfer of PNR data the European Union and the United States declare the information sharing as an essential component in the effective fight against terrorism and transnational organised crime – in this PNR data is found as an important tool. Article 8 of the European Convention on Human Rights constitutes that the intrusion in the right to respect for private life by state authorities to be considered lawful requires to be necessary in the democratic society and justified by the interests of inter alia national security and public safety. The limitation of individual's privacy must be consistent with the principle of proportionality stated in the Convention No. 108 and the Directive 95/46/EC. The requirement of proportionality was reapeated in the Council Framework Decision on the protection of personal data in the framework of policy and judicial cooperation in criminal matters. Considering the potential impact on the fundamental rights of the European citizens and bearing in mind the massive expenses of the air carriers, the effectiveness and the added value of PNR data processing in the combat againt terrorism was called in question.

The European Parliament in the resolution of 20 November 2008 reminded that the justification of the proposal for every new legal act to be adopted should be convincingly substantiated – the information provided to the Member States authorities as well as to the Parliament itself must be even more detailed and complete by the measures which create higher risk of violation of the fundamental rights. Therefore, it is suprising that neither the European Parliament[85], nor the the Article 29 Working Party, Fundamental Right Agency and the European Data Protection Supervisor had received complete information or convincing evidence on effectiveness and pressing need of PNR data processing in preventing and combating terrorism or organised crime as well as on insufficiency of existing legal measures including Directive 2004/82/EC on the obligation of air carriers to transmit API data to the Member States' border control authorities. Hitherto the European Commision exemplify the added value of PNR data with the experiences of the United States and the United Kingdom's pilot project Semaphore (a part of e-Boarders Programme) in the use of PNR data in criminal investigations. At the tripate meeting in Berlin in April 2007 between the United States and the Commision and in the letter from the Secretary of Homeland Security to Members of the European Parliament on 14 May 2007 the examples of security achievements, which were the results of PNR data processing, were presented – it is to be stated, that in the opinion of the British parliamentarian, the examples of the use of PNR data weren't sufficient enough to enable them to assess the value of such data.[86] Other information on the use of PNR data in criminal investigation were strictly confidential as the policy and judicial authorities are reluctant to provide information concerning the investigating methods. According to the information provided by Joan Ryans (the Parliamentary Under-Secretary of State) the United Kingdom's project Semaphore, which use PNR data for automated profiling, was successful in combating illegal immigration and serious crimes.[87] However, there was no evidence, that

---

[84] Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes.

[85] Resolution of the European Parliament of 12 July 2007 p.28.

[86] *The US/EU Passenger Name Record (PNR) Agreement. Report with evidence*, House of Lords – European Union Committee, 21th Report of Session 2006-2007.

[87] op.cit.

Semaphore may be useful as counter-terrorist measure.

Referring to the opinion of the Article 29 Working Party adopted in 2007[88], the evaluation of the necessity of PNR data processing in fighting against terrorism is not possible, even compared with a similar measures established on the grounds of Directive 2004/82/EC. The abovementioned Directive forsees the obligation on air carriers to collect and transmit the API data in order to fight illegal immigration. The Directive is not yet fully in force thus the analysis of effectiveness of processing data can't be carried out. The Working Party rightfully remarked that the intruducing of more intrusive means, before proving the effectiveness of API data processing is deprived of justification. Fundamental Rights Agency shared this statement in its opinion on the proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes from 2008.

In conclusion it is to be stated, that more explanation should be provided to the public in order to demonstrate beyond doubt the pressing need for collecting and sharing PNR data with the United States. The Privacy International organisation in its report on transfer of PNR records raised an objection of „policy laundering" to the European Commission.[89] Policy laundering is a term used to describe the usage of the requirements of other state's jurisdiction as justification to obtain or enhance powers or means unobtainable on the basis of own law. The Privacy International suggests that the European Union aim is to establish an European surveillance system on the grounds of the Agreement and further counter-terrorist cooperation with the United States. The similar doubts were expressed in the opinion of the Article 29 Working Party.[90]

7.7.1 The types PNR data to be collected

The explanatory letter of the Secretary of Homeland Security specifies 19 PNR data elements to be collected and transferred to the Department of Homeland Security and to the U.S. agencies. Refering to the first Agreement between the European Union and the United States the number of elements was reduced from 34 to 19 types of data, the reduction though is only illusive. The Article 29 Working Party rightfully highlighted that the list from the new Agreement contains all 34 types of data required on the basis of previous regulation – some of the elements were put together in order to conceal the fact, that in reality it is not 19 elements, but 34.[91] Moreover comparing to the Agreement from 2004 the variety of elements to be transmitted to DHS was increased due to more general form of describing the types of collected information – it entitles to demanding all detailed information that may come under the defined type of PNR data, while the scope of the information in the Agreement from 2004 was limited to precisely described types of PNR data. As a result the amount of PNR data is very wide and to excessive in the relation to the purpose the data are collected. The Working Party, substantiating the need to curtail the abovementioned list, reminded that the Department of Homeland Security has other sources of personal information in his disposal such as personal data required for immigration formalities, transmitted via API system etc.[92] In conclusion the principle of proportionality regarding the list of PNR data collected is to be questioned.

---

88 The Article 29 Working Party, joint opinion on the Proposal for Council Framework Decision on the use of Passenger Name Record for law enforcement purposes adopted on 5 December 2007.

89 *Transferring Privacy: The Transfer of Passenger Name Record and the Abdication of Privacy Protection. The first report on „Towards an International Infrastructure for Surveillance of Movement"*, Privacy International, February 2004.

90 The Article 29 Working Party, joint opinion on the Proposal for Council Framework Decision on the use of Passenger Name Record for law enforcement purposes adopted on 5 December 2007.

91 The Article 29 Working Party, opinion 5/2007 on the follow-up agreement between the European Union and the United States on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security concluded in July 2007.

92 The Article 29 Working Party, opinion 4/2003 on the level of protection ensured in the US for transfer of passengers' data adopted on 13 June 2003

7.7.2 Sensitive data and the right to privacy of third persons

Article 6 of the Council Framework Decision 2008/977/JHA distinguishes the special category of personal data – so-called sensitive data. The definition of sensitive data mirrors the regulation of the Directive 95/46/EC accorrding to which sensitive data are defined as personal data revealing racial or ethnic origin, religious or philosophical beliefs, or trade union membership (...), data concerning health or sex life. The PNR Agreement doesn't include *expressis verbis* the sensitive data to be collected, but such data might be contained in free text fields like "general remarks" or "historical changes in PNR". The Article 29 Working Party in the opinion from 2002 noted that the information in free text field may reveal religious or ethnical origin (choice of meal, place of residence), affiliation to any particular group or medical data (any medical assistance required, oxygen, problems relating to sight, hearing or mobility or any other problem which must be made known to ensure a satisfactory flight).[93] The processing of such data is in principle prohibited – both Directive and the Council Framework Decision provide special cases and requirement when the exception to that prohibition is possible and lawful. The exception can be made only if the national law provide adequate safeguards and the processing of sensitive data is strictly necessary. The letter of the Secretary of Homeland Security ensures that the sensitive data will be filtered and deleted, but also establishes additional cases, when the prohibition on processing of sensitive data can be lifted:

„in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired, DHS officials may require and use information in EU PNR other than those listed above, including sensitive data. In that event, DHS will maintain a log of access to any sensitive data in EU PNR and will delete the data within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law. DHS will provide notice normally within 48 hours to the European Commission (DG JLS) that such data, including sensitive data, has been accessed."

The abovementioned provision is unacceptable on the grounds of the European Union data protection law.

The abovementioned regulations of the Agreement include exception from the prohibition of the automathic processing of sensitive data, that can not be considered lawful on the grounds of European data protection law. The exception in the letter of the Secretary of Homeland Security creates additional circumstances, that justify the collection of sensitive data – the abomentioned Directive 95/46/EC includes the numerus clausus of cases, to which the prohibition of processing of sensitive data doesn't apply, thereby any processing of sensitive data that is not consistent with the exceptions in the Directive must be considered as a violation of law. The catalogue of exceptions to prohibition of processing of sensitive data can not be extended due to the specific nature of such data – the informations revealing the ethnic or national origin, sexual preferences, religious or philosophical beliefs or state of health affect the most intimate sphere of individual's privacy and as a consequence must be under special protection. According to the Council Framework Decision 2008/977/JHA the processing of the special cathegory of data must be strictly necessary. The stipulations of the Agreement describe the exceptional cases very broadly, which may be dubious in the light of the principle of proportionality. Furtermore the Agreement ensures DHS the access to **any** sensitive data, creating a serious risk of misuse of authority and violation of passengers' fundamental rights by U.S. Department of Homeland Security and U.S. agencies entitled to receive PNR data. Such encroach in individual's privacy can not be justified on the ground of European Community law and Article 8 of the European Convention on Human Rights.

The European agencies engaged in the data protection rightfully questioned the method

[93] The Article 29 Working Party, opinion 6/2002 on the transmission of Passenger Manifest Information and other data from airlines to the United States adopted on 24 October 2002.

of data filtering. Point III of the explanatory letter cedes the responsibility for filtering sensitive data on the DHS – the sensitive data will be filtered by the means of trigger terms of codes. This method must be considered ineffective - the Article 29 Working Party pointed out, that the notion and relevance of personal data as sensitive changes over time, which imposes the continous improvement of the filtering system[94] as well as the verification and supplementation of existing terms and codes. This approach may not guarantee the deletion of all sensitive data.

The PNR data (for example "all available contact information" or "all available payment/billing information") may also contain the information on third parties like the employer, partner or relatives. The third party in most cases won't be aware of the processing and transfer of personal data and therefore won't exercise his or her rights.[95]

7.7.3 The system of transferring PNR data – "push" and "pull" method

One of the most discussed matter concerning the air carriers obligation of transmitting PNR data to the U.S. Department of Homeland Security was the method of personal data transfer. In PNR transfer regime two methods of trasmission are possible – the "pull" system ensures the recipient (DHS) direct online access to air carriers' reservation system and databases; the "push" system leaves the responsibility for selecting, filtering and transmitting certain types of personal data by the airlines.

From the beginning of the negotiations with the European Union, the United States contracting party forced the implementation of "pull" method that ensured the unlimited access to airlines' databases – the filtrating process were conducted inside the DHS's operating system. It is to be mentioned, that the filtering system providing filtering of sensitive data and data beyond the permitted 34 elements was implemented on 14 March 2005[96] – almost a year after signing the first Agreement on PNR processing. The Article 29 Working Party in the opinion of 22 June 2004 underlined that the general principle of data protection law limits the scope of transmitted data to those the recipient actually needs[97] – the "pull" method opposes this principle. In its application in the joined cases C-317/04 and C-318/04 in the European Parliament's opinion the term "data transfer to third countries" on the basis of the Directive 95/46/EC does not include "pull" method – the European Parliament defined "pull" method as a direct download of personal data inadmissible on the grounds of the abovementioned Directive. The Article 29 Working Party shared the opinion of the European Parliament considering the "push" method the only system of transferring PNR data that is in line with principle of proportionality and ensures the liability of data controller established by the Directive 95/46/EC – after the annulment of the EU-US Agreement from 2004 the Working Party repeatedly insisted on implementation of "push" method of transmitting PNR records to the Department of Homeland Security.[98]

---

94 The Article 29 Working Party, joint opinion on the Proposal for Council Framework Decision on the use of Passenger Name Record for law enforcement purposes adopted on 5 December 2007; The Article 29 Working Party, opinion 5/2007 on the follow-up agreement between the European Union and the United States on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security concluded in July 2007.

95 op.cit.

96 Commission Staff Working Paper on the joined review on the implementation by the U.S Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC on 14 May 2004, redacted version from 2005.

97 The Article 29 Working Party, opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.

98 The Article 29 Working Party, opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States; The Article 29 Working Party, opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the UnitedStates and the urgent need for a new agreement

In the final text of the existing Agreement on PNR processing the contracting parties adopted the regulation burdening the air carriers with the duty of transition to "push" system. The "pull" system remains in effect for those of the air carriers, who failed to implement the "push" system that complies with DHS's technical requirements before 1 Januray 2008. The existence of the both methods was questioned in the light of distortion of competition between the air carriers. The modification of transferring method should be considered a satisfactory change in comparison to the former Agreement, nonetheless the regulation in this matter needs further improvement. Although the method of the transfer was modified, the decision on frequency and scope of transmitted PNR information is conferred on DHS. The Article 29 Working Party underlined that the number of data updates shouldn't be a one-sided decision of the DHS – instead the Working Party suggests adopting the provision limiting the number of push requests.[99]

In conclusion, the opinion of air carriers in that matter should be presented as well, considering that it is the airlines, who will be responsible for implementing the modified data transfer system. In the memorandum, the British Air Transport Association opted for the "push" method as it provides "an advantage to the carrier in that carriers have some control over costs".[100]

7.7.4 Obligation for air carriers

According to the paragraph 2 of the US-EU Agreement, the pull method of PNR data transfer will apply to air carriers that have implemented such a system that complies with DHS's technical requirements. The explanatory letter of the Secretary of Homeland Security includes a regulation according to which, the responsibility for initiating the transition to "push" system rests with the air carriers. The Agreements doesn't include any references concerning who should bear costs of adaptation of the air carriers' systems to DHS standards, which means the air carriers will be burdened with expenses - the British Air Transport Association submitted a written evidence to the House of Lords, in which the Association presented an opinion, that „the costs should lie with the requesting authority". The European Travel Agents' and Tour Operators' Associations in the letter to the Council of the European Union of 1 August 2008 pointed out, that the costs would inevitably be passed on by the carriers to the end user – the passengers. The Statewatch Observatory concluded, that the passengers will be paying for their own surveillance and inconveniences resulting from the implementation of the PNR processing system.[101] Furthermore the obligation for air carriers to implement the new PNR system and the short time period for complience will result in existence of two methods of PNR data transfer, which can cause the distortion of competition between the European air carriers.[102]

8. Passenger Name Record as an evidence in criminal proceeding

The third pillar of the European Union creates the ground for cooperation in criminal matters for the Member States. The tragic events on 11 September 2001 highlighted the inadequacy of existing legal means in fight against terrorism and the pressing need for cooperation on global level. At the extraordinary meeting on 21 September 2001 the European Council declared fight against terrorism a priority objective to the European Union – this statement was followed by a declaration that the European Union would support the international community in its combat

---

[99] The Article 29 Working Party, opinion 5/2007 on the follow-up agreement between the European Union and the United States on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007.

[100] Memorandum of BATA, written evidence supplementing *The US/EU Passenger Name Record (PNR) Agreement. Report with evidence*, House of Lords – European Union Committee, 21th Report of Session 2006-2007.

[101] http://www.statewatch.org/news/2008/aug/eu-pnr-ectaa-comments.pdf.

[102] Michele Nino, *The protection of personal data in fight against terrorism. New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon*, Utrecht Law Review 6/2010; resolution of the European Parliament of 12 July 2007; see also opinion of the Advocate Generale P. Légere of 22 November 2005 according to joined cases C-317/04 and C-318/04.

against terrorism in every shape and form[103] – the great emphasis was placed on cooperation with the United States. The Agreement between the European Community and the United States of America on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security from 2007 was established as an element of cooperation in criminal matters, complementary to the Agreement on mutual legal assistance from 2003.[104]

8.1 The purpose of PNR processing

The Agreement consists of the document of the agreement itself and the explanatory note in a letter of Secretary of US Homeland Security. The preamble of the Agreement stresses the importance of preventing and combating terrorism and related crimes as well as other serious crimes organised and transnational in their nature. The letter specifies the purpose of processing PNR data to fighting and preventing „(1)terrorism and related crimes, (2) other serious crimes including organised crimes that are transnational in nature and (3) flight for warrants and custody for crimes described above. The PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law". Refering to the aforementioned remarks on excessively broad scope of crimes formulated in the Agreement it is to be assumed that the indicated legal purpose of PNR processing is carrying out risk assessment of passengers by creating a profile of such person (profiling), obtaining intelligence and making associations between known terrorist and their unknown accomplice (identyfing the structure of terrorist organisation[105]) and identyfing terrorist before the execution of planned terrorist act.

8.2 PNR profiling and the its impact on individuals

The PNR processing system was established to create profiles of the terrorist and their associates on basis of PNR provided by air carriers and travel patterns and other trends characteristic for persons involved in organising terrorist attacks and organised crimes. „Profiling" is generally defined as the systematic association of sets of physical, behavioural or psychological characteristics with particular offences such as terrorism.[106] Profiling can be either descriptive (identification of persons who are suspected to have commited terrorist offence; PNR becomes a corroborating evidence or condradicts already gathered information) or predictive (identification of a person involved in planned but not yet commited offence; preventive function of PNR data). Terrorist-profiling, particularly in its predictive form, may violate the prohibition of dicrimination on grounds of race, ethnic or national origin or belief and thereby be infringement of Article 21 of the Charter of Fundamental Rights of the EU. The added value of PNR is a possibility to compare data related to known terrorist (travel routes, travel history) and data of individuals who are not yet linked with terrorist groups. The reports of organisations fighting against discrimination[107] reveal that counter-terrorist profiling are usually based on stereotypical assumption and wrongful generalisation. Relying on ethnic or national origin, passengers who come from countries that are considered „state sponsors of terrorist" or „countries of interest" are percept as supporters or even members of terrorist groups which derive from this state or are active on its territory. Such passengers are often treated not as individuals, but as a members of a group, taking the consequences of terrorist action and being stigmatized as members of targeted ethnical or national group. Refering to the article published on The New York Times on 3 January 2010 the

---

[103] Council Common Position on 27 December 2001 on combating terrorism (2001/930/CFSP) O.J. L 344/90

[104] O.J. L 181/34.

[105] Kazimierz Olejnik, *Problematyka dowodowa przestępstw o charakterze terrorystycznym oraz efekty czynności operacyjnych*, Prokurator 4(28)/2006.

[106] Opinion of the European Union Agency for Fundamental Rights on the proposal for a Council Framework Decision on the use of Passenger Name Record data for law enforcement purposes.

[107] European Network Against Racism, European Council on Refugees and Exiles, European Monitoring Centre on Racism and Xenophobia, Open Society Institute.

Transportation Security Administration decided that citizens of „14 countries of concern" will be experiencing special, detailed scrutiny on airports.[108] In the letter of Secretary of Homeland Security specified personal data revealing racial or ethnic origin, political opinions, religious or philosophical belief etc. (sensitive data) are to be deleted, unless they are accessed for an exceptional case when the life of a data subject or others are imperilled or seriously impaired. According to European Data Protection Supervisor[109] „although it cannot be assumed that passengers would be targeted according to their religion or other sensitive data, it appears nevertheless that they would be subject to investigation on the basis of a mix of *in concreto* and *in abstracto* information, *including* standard patterns and abstract profiles" which would be not only violation of respect for individual's right to privacy, but also it would be an infringement of prohibition of discrimination guaranteed by Article 21 and 52 of the Charter of Fundamental Rights and by Article 14 of the European Convention on Human Rights. Such use of PNR data is unacceptable as undermining the values on which the European Union was established and *per se* unlawful. Furthermore the use of PNR data to counter-terrorist profiling negates the presumtion of innocence guaranteed in Article 48 of the Charter of Fundamental Rights and Article 6 of the European Convention on Human Rights. In the name of fighting and preventing terrorism thousands of people annually might be affected by suspicion of belonging to an organised criminal group or terrorist organisation on the ground of being a member of certain ethnic group or because of identity of his/her travel history with the travel pattern of a terrorist.

8.3 The value of PNR evidence

According to the Council Framework Decision on the execution in the European Union of orders freezing property or evidence (2003/577/JHA) "evidence" shall mean objects, documents or data which could be produced as evidence in criminal proceedings concerning among other offences also terrorism.[110] The Council Framework Decision of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (2008/978/JHA) specifies evidence as "any objects, documents and data for use in proceedings in criminal matters for which it may be issued. This may include for example objects, documents or data from a third party, from a search of premises including the private premises of the suspect, historical data on the use of any services including financial transactions, historical records of statements, interviews and hearings, and other records, including the results of special investigative techniques.[111] On the ground of European legislation PNR data can become an evidence in criminal proceeding. The formalities and procedures concerning taking the evidence of PNR before the court are to be conducted regarding to the criminal procedure of the Member State.

The rules of evidence for the United States were adopted by Congress in 1975 in the Federal Rules of Evidence act. According to the Rule 401 and 402 "relevant evidence means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence" and "all relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible".[112] Those rules should be supplemented by the doctrine of "fruit of the poisonous tree" which prevents evidence obtained illegally from being admitted in a criminal trial. With the abovementioned rules in mind it

---

[108] Eric Lipton, *U.S. intensifies air screening for fliers from 14 nations*, The New York Times from 3 January 2010.

[109] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, O.J. C 110/1.

[110] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, O.J. L 196/45.

[111] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, O.J. L 350/72.

[112] *Federal Rules of Evidence* published by Legal Information Institute of Cornell Univeristy Law School on December 2009.

is admissible for PNR data to become an evidence in criminal proceeding before the U.S. courts.

In the light of above described potential negative impact on large number of passengers crossing the Atlantic and serious threat of violation of the prohibition of dicrimination and right to privacy, the value of PNR data as an evidence in criminal proceeding is called in question. Thus far, the European Commission has neither presented the convincing proofs of the added value of PNR data in combating terrorism, nor it has proved the insufficience of existing measures for law enforcement purposes such as VISA Information System or API processing on the basis of Directive 2004/82/EC. The pressing need for available information on effectiveness of PNR data processing for purposes of combating terrorism and organised crime was repeatedly empasized in opinions of both Article 29 Working Party as well as the European Union Agency for Fundamental Rights.[113] The fragmentary information refering to the positive experiences of third countries such as Canada and the United States in the use of PNR data in criminal investigations as well as to United Kingdom's pilot project "Semaphore" were questioned in the Open Society Justice Initiative's report[114] – it showed that counter-terrorist profiling practices were scantly effective in detecting terrorist crimes and so, they have little value as evidence.

It must be stressed that PNR data in the penal proceeding shall be used as an circumstantial evidence and substantiated with furter, directive evidences. PNR data provide information regarding the potential terrorist association of a passenger and identify the connection between travel routes of a passenger and the terrorist activity in the state of individual's travel destination. Nevertheless PNR data can not be considered as an sufficient incriminating evidence that unequivocally determines the perpetration or aiding and abetting of a defendant – Passenger Name Record only substantaties the guilt of the execution or preparation of of terrorist attack. The profiling on the basis of PNR data and the application of penal measures as well as the effect of the PNR processing system resembles the operation of a fishing trawler – the retrieval of significant information by means of collecting, filtering and analysing of a vast amount of personal data which generates the high expenses for both air carriers and the European Union with a scant value of collected records for criminal proceeding.

Regarding the arguments above, it is to be stated that the significance of PNR data as evidence in penal proceeding is disproportionate to the expected effects for the fight against terrorism and organised crime, expenses and the threat to fundamental rights.

9. Conclusion

The terrorist attack on 11 September 2001 against the United States and the following attacks in Europe changed the view on a phenomenom of terrorism. Terrorism was declared one of the greatest threats to public security, democratic society, peace, stability and fundamental rights - values on which the European Union as well as the United States were founded. In the aftermath of tragic events in the USA the Member States realised the terrorism is neither a temporary phenomenom nor the problem of a single nation, but over the years it has grown into well-organised, transnational threat that should be unequivocally condemned and overpowered with all available means. The Member States also perceived the necessity of international cooperation in this matter – both in its European harmonisation aspect as well as in the transatlantic dimension. The legal measures as a response to terrorist threat were the matter of a heated discussion on both EU level as on the level of single Member States. Nevertherless the complexity and the diversity of

[113] A Common Approach to the use of PNR data for law enforcement purposes: Impact Assessment Questionnaire to data protection authorities – Joint answer of Article 29 Working Party;
Opinion of the FRA on the proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes.

[114] *Ethnic Profiling in Europe: Counter-Terrorism Activities and the Creation of Suspect Communities*, Open Society. Justice Initiative, June 2007.

an organised crime and the offences that might come under the definition of terrorism became a difficulty in context of creating the legal definition of the terrorism likewise it called into question the effectiveness of proposed instruments. Neither the international legal instruments adopted under the auspices of the United Nations, nor the framework decision of the European Council on 13 June 2002 concerning the fight against terrorism and later the Guidelines on human rights and the fight against terrorism adopted on 11 July 2002 by the Committee of Ministers[115] have really succeeded in overcoming those difficulties – the aforementioned legal acts only set up a general frame for future legal instruments. Most of legal instruments suggested or even passed in the Member States were questioned in context of civil liberties, constitutional guarantees or fundamental rights[116]. It was reminded that the state authorities cannot combat terrorism or organised crime guided by the rule of fighting fire with fire with disregard of the existing international commitments as well as domestic law – the fundamental values the terrorist and others advocating the use of violence seek to destroy[117].

Among discussioned measures, the Member States of EU and the United States realised the value of collecting and analysing personal data which were already collected by air carriers for their commercial purposes and for the purposes of fighting illegal immigration (APIS system established in directive 2004/82/EC) as a tool in combating and preventing acts of terrorism.

In the context of processing personal data, the remark of Professor Marek Safjan considering electronic personal data a double-edged sword remains valid[118]. At the present times it is almost impossible for an individual to function in modern society without giving access to his or her personal data – the citizen is a beneficiary of the global network system, but he might become as well its victim in case of violation of his right to privacy or misuse of this data. Since the scope of individual's right to privacy is nowadays drawn not by the authonomy of data subject, but by the interest of others, it is the duty of the authorities to balance the public interest (need for security) and the private interest of each member of society (respect for privacy of individual). The case of PNR Agreement between the United States and the European Union portrays all the difficulties the states are to face in the course of enacting legal instruments which will become an effective response to terrorist threat.

Aforementioned doubts concerning the lawfulness of provisions incorporated in the Agreement reveals the imperfection of this legal act. It is dissatisfied that since 2007 – the year the Agreement was concluded – the Commission didn't take any measures to change the current state. It is to presume the inactivity in this matter is a result of lack of Commission's political will and the specific geopolitical situation both of contracting parties had to face – the military operation in Iraq and the different attitude to military engagement the Member States were presenting, the presidential election in the USA, the adoption of the Lisbon Treaty and new Member States. However, the repeated accusations of „trading freedom for security”[119] in media releases and critical voices of law community and international institutions engaged in personal data protection and protection of human rights[120] is sufficient reason for the Commission to take action in this matter.

In conclusion it is expected from the Commision in cooperation with the United States authorities to undertake the following measures:

---

[115] Guidelines on human rights and the fight against terrorism adopted by the Committee of Ministers on 11 July 2002 at the 804th meeting of the Ministers' Deputies, Directorate General of Human Rights, December 2002

[116] See for example: judgement of Polish Constitutional Tribunal from 30 September 2008, signature K 44/07; judgement of Federal Constitutional Tribunal of Germany (Bundesverfassungsgericht) from 15 February 2006, signature 1 BvR 357/05; widely about the economical sanctions against individuals accused of terrorism activity and violation of fundamental rights – Joanna Ryszka, *Ochrona praw podstawowych a sankcje UE stosowane w walce z międzynarodowym terroryzmem*, EPS 11/2008.

[117] Opinion 10/2001 of Art.29 Data Protection Working Party *on the need of a balanced approach in the fight against terrorism adopted* on 14 December 2001.

[118] Marek Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, PiP 6/2002.

[119] Term used in article *Trading freedom for security* in The New American Magazine on 5 May 2003.

[120] Among them: European Data Protection Supervisor, Article 29 Data Protection Working Party, Statewatch, European Union Agency for Fundamental Rights, Electronic Privacy Information Center.

- eliminate imprecise and open-ended formulation so that the regulations of the Agreement reach the adequate degree of certainty and forseeability
- reduce the real amount of collected PNR
- specify the US agencies legitimate to receive PNR from European air carriers
- changing „pull" to „push" method of transfering PNR to DHS
- specify the procedure of joint review of the Agreement
- establish the institution responsible for data processing and transfering personal data to the US agencies (Passengers Information Unit)
- specify the subjects responsible for informing passengers on PNR processing and means of appeal passengers are entitled to in context of PNR processing (sufficient procedural safeguards)
- reduce the data retention period and exceptions in this matter
- change the method of collecting and filtering sensitive data to reduce the threat of violation of right to privacy of PNR subjects
- specify the purpose the PNR are to be used with special attention to using PNR in penal proceedings
- provide more explanation and evidence on necessity of establishing new system of PNR processing and on insufficiency of current measures in fight against terrorism
- ensure that data transfers are possible only to third countries that guarantee the adequate level of protection and can be monitored in recipient country

In conclusion it is worth reminding that every new legal instrument expanding the scope of surveillance and invasing the privacy of the individuals should meet the requirements of protection of the fundamental rights in democratic society. The implementing of PNR collecting system may generate the risk of undermining the democratic society in the name of protecting it. With the above in mind the Member States and the European Union should persistently aim to improve the existing legal instruments of protection against organised crime and terrorism instead of representing the protection of personal data and right to privacy as a barrier in efficient crusade against terrorism.