

MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
INSTITUTE OF INTERNATIONAL AND EUROPEAN UNION LAW
&
UNIVERSITÉ DE BORDEAUX
FACULTY OF LAW

EGLĖ BEINORYTĖ
(JOINT EUROPEAN UNION LAW AND GOVERNANCE PROGRAMME)

LEGALITY OF EUROPEAN UNION'S BILATERAL PNR AGREEMENTS WITH NON-
EUROPEAN UNION COUNTRIES

Master thesis

Supervisor

Prof. dr. Regina Valutyte

Vilnius, 2016

TABLE OF CONTENTS

ABBREVIATIONS	3
INTRODUCTION	4
I. GENERAL CONCEPTS AND THE NEED FOR EU BILATERAL PNR AGREEMENTS	11
1.1. Concept of API and PNR data.....	11
1.2. The need for EU bilateral PNR Agreements with non-EU countries.....	13
1.3. EU PNR directive.....	19
II. FUNDAMENTAL HUMAN RIGHTS STANDARDS APPLICABLE FOR THE ASSESSMENT OF PNR AGREEMENTS	22
2.1. Data protection regulations ascertained in the EU	23
2.2. The origins of EU data protection law applicable to assess PNR Agreements	25
2.3. Joint Reviews of the PNR Agreements	35
III. THE COMPATIBILITY OF THE EU-CANADA, EU-USA AND EU AUSTRALIA PNR AGREEMENTS WITH THE EU PRIVACY AND DATA PROTECTION RULES	42
3.1 Necessity of the PNR agreements concluded by EU with Canada, USA and Australia	43
3.2. Proportionality of the PNR agreements concluded by EU with Canada, USA and Australia	44
3.2.1. Proportionality of the use of PNR data ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements.....	45
3.2.2. Proportionality of the data elements to be collected ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements	52
3.2.3. Proportionality of the data retention periods ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements.....	60
3.2.4. Proportionality of the disclosure of data ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements	69
3.2.5. Proportionality of the guarantees for and rights of data subjects ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements	77
CONCLUSIONS AND PROPOSALS.....	87
BIBLIOGRAPHY	90
ANNOTATION	102
ANOTACIJA	102
SUMMARY	104
SANTRAUKA	105
ANNEX.....	108
CONFIRMATION OF INDEPENDENCE OF THE WRITTEN WORK.....	111

ABBREVIATIONS

API data- Advance Passenger Information data

PNR data - Passenger Name Record data

EU- the European Union

USA/US – the United States of America

ATSA - Aviation and Transportation Security Act

CBSA - Canada Border Services Agency

CJEU – the Court of Justice of the EU

Charter- the Charter of Fundamental Rights of the European Union

Convention/ECHR - Convention for the Protection of Human Rights and Fundamental Freedoms

ECtHR – the European Court of Human Rights

ACS - Australian Customs Service

PIU - Passenger Information Unit

The Art. 29WP - the Article 29 Data Protection Working Party

TFEU - the Treaty on the Functioning of the EU

ACBPS - the Australian Customs and Border Protection Service

EDPS - the European Data Protection Supervisor

INTRODUCTION

The problem examined in the thesis and the relevance of the thesis. In recent years, the global community has witnessed a tremendously growing wave of terrorism attacks¹ and serious transnational crimes². The contemporary developments in technology have given the access to transfer vast amounts of personal information of individuals.³ As a matter of fact, the twenty first century states, individuals and companies are taking precautions when it comes to collection, handling, transferring of their private or personal data. Constantly increasing transnational crime rate called for new technological developments in the society to be used as a tool to fight this cross-border phenomenon.⁴

Passenger Name Record (PNR) data, which is unverified information submitted by travelers upon reservation of an airplane ticket and held in the carriers' reservation system⁵, is currently viewed as one of the key tool in the fight against terrorist offences and serious transnational crimes. However, the processing of such data poses a serious threat to the respect for fundamental rights of individuals, especially the right to respect persons' private life and the right to the protection of personal data.

Although the use of PNR data has become harmonized at the European Union (hereinafter EU) level by adopting EU PNR Directive on the 27 of April 2016, the use of PNR data is not currently harmonized at the international level. Meanwhile, after 9/11 attacks in the United States of America (hereinafter USA) a number of non-EU countries started to require air carriers arriving at their territory to submit PNR data. USA, Canada and Australia were among those countries. Therefore, EU was confronted with the urgent choice of either facing heavy fines/ loss of the landing rights in

¹ Dov Waxman, "Living with terror, not Living in Terror: The Impact of Chronic Terrorism on Israeli Society", *Perspectives on terrorism*, Vol 5, No 5-6 (2011), ISSN 2334-3745 (Online), [last accessed 12-25-2016] <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/living-with-terror/html>.

² Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SEC(2011) 133 final}, p. 2.

³ The Commissioner for Human Rights, "Rights Protecting the right to privacy in the fight against terrorism", CommDH/IssuePaper(2008)3, Strasbourg, 4 December 2008 pp. 4

⁴ Proposal for a Directive on the use of Passenger Name Record data, op. cit., p.3.

⁵ International Civil Aviation Organization "Guidelines on Passenger Name Record (PNR) data", Approved by the Secretary General and published under his authority, First Edition — 2010, pp. 2.1.1, see also Proposal for a Directive on the use of Passenger Name Record data, op. cit., p.3.

the territories of the countries or potentially infringing EU data protection laws⁶ as laid down in the EU Data Protection Directive 95/46/EC.⁷ Therefore, to comply with requirements and to increase international cooperation in the area of fight against terrorism and serious transnational crimes, the EU concluded first Agreements on the processing and transfers of EU-sourced PNR data with USA in 2004⁸, with Canada in 2006⁹ and with Australia in 2008¹⁰. Following the entry into force of the Lisbon Treaty, the PNR Agreements between the EU-USA, EU-Canada and EU-Australia were renegotiated. Both newly renegotiated PNR Agreements with USA and Australia went into force in 2012.¹¹ This was not the case with newly renegotiated 2014 EU PNR Agreement with Canada.¹² EU Parliament before giving its consent to conclude the Agreement brought a case before the Court of Justice of the EU (hereinafter CJEU) to assess the compatibility of the 2014 PNR Agreement regarding rights guaranteed under EU treaties, in particular the rights to privacy and data protection.¹³ As of 31 December 2016 the case is still pending in Court. Irrespective of its content, the Court's answer to the request of European Parliament may have implications for the PNR Agreements already in force between the EU and Australia and the EU and the United States of America.¹⁴ Often described as the "least intrusive" PNR agreement, the shortcomings of the EU-Canada agreement may put into question the validity of all existing PNR agreements and of the EU

⁶ Hobbing, P, "Tracing Terrorists: The EU-Canada Agreement in PNR Matters", CEPS Special Report/September 2008, p. 10

⁷ Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004.

⁸ 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 O.J. (L 183) 84-85 [hereinafter 2004 EU-USA PNR Agreement].

⁹ Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJL 82, 21.3.2006. [hereinafter 2006 EU-Canada PNR Agreement]

¹⁰ Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the EU, of an Agreement between the EU and Australia on the processing and transfer of EU-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, OJL 213, 8.8.2008, p. 47. [hereinafter 2008 PNR Agreement].

¹¹ Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, [hereinafter 2012 EU-USA PNR Agreement] see also Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, L 186, 14/07/2012, [hereinafter 2012 EU-Australia PNR Agreement] p. 4, pp. 1

¹² Proposal for a Council Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013) 529final, Annex Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data, [2014 EU-Canada PNR Agreement], pp.3.

¹³ Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU, Opinion 1/15, 2015/C 138/32.

¹⁴ Opinion 1/15 of Advocate General Paolo Mengozzi, ECLI:EU:C:2016:656, pp. 4

PNR Directive.¹⁵ In the light of upcoming judgement of the CJEU on the 2014 EU-Canada PNR Agreement closer look must be taken to all the PNR Agreements concluded by EU with non-EU countries. In particular, compatibility of the existing scheme of PNR Agreements with the primary law of EU and its actual added value to prevent and combat terrorism and serious transnational crimes.

Although data and privacy protection is often seen as an obstacle to effective anti-terrorist measures, it is crucial to the upholding of fundamental democratic values.¹⁶ This tension between strong opposing forces, the desire to preserve fair balance between the legitimate desire to maintain public security and the equally fundamental right for everyone to be able to enjoy a high level of protection of his private life and his own personal data is the **main problem dealt with in the thesis**.

Review of the literature, novelty and originality of the thesis. The research on PNR Agreements lacks the attention of foreign scholars. In particular, very little has been written about EU-Australia PNR Agreements. Even though EU-USA and EU-Canada PNR Agreements has been given considerably more attention most provisions are discussed rather briefly. Such scholars as, for instance, D. Louks¹⁷, R. Koslowski¹⁸, P. Hobbing¹⁹, M. Nino²⁰, F. Rossi Dal Pozzo²¹, Kaunert, S. Leonard and P. Pawlak²², C. Blasi Casagran²³, E. Guild and E. Brouwer²⁴ provide rather brief analysis of PNR Agreements' provisions. Considerable amount of criticism was directed to rather long period of data retention, wide spectrum of data processing purposes, a large amount of data

¹⁵ Estelle Massé, "Advocate General opinion on EU Canada PNR agreement: it won't fly", 8 September 2016, <https://www.accessnow.org/advocate-general-opinion-eu-canada-pnr-agreement-wont-fly/> [last accessed 11.24.2016]

¹⁶ The Commissioner for Human Rights, *supra* note 3, pp. 3.

¹⁷ Louks, D., "(Fly) Anywhere but here: approaching US-US dialogue concerning PNR in the era of Lisbon", *Int'l & Comp. L. Rev.* 479 2013.

¹⁸ Kozlowski, R., "Border and Transportation Security in the Transatlantic Relationship", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London/New York, 2006, pp. 89–105, p. 80

¹⁹ Hobbing P., "Tracking Terrorists: The EU-Canada Agreement in PNR Matters" *supra* note 6, p. 10.

²⁰ Nino, M., "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* 62 2010, pp. 62

²¹ Rossi Dal Pozzo, F., "EU Legal Framework for Safeguarding Air Passenger Rights", Springer International Publishing Switzerland 2015, p. 119

²² Kaunert, C., Leonard, S. and Pawlak, P., *Contemporary Security Studies, European Homeland Security– A European Strategy in the Making?*, MacKenzie, A. "The external dimension of European homeland security", p. 95 -111, First published 2012 by Routledge 2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN. p. 103

²³ Blasi Casagran, C., "Global Data Protection in the Field of Law Enforcement– An EU Perspective", Routledge Taylor & Francis Group, London and New York, 2017. p. 110

²⁴ Guild, E. and Brouwer, E., "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US", CEPS Policy Brief No. 109, CEPS, Brussels, 26 July 2006.

elements to be collected, disclosure of data to other government authorities and third countries and guarantees for and rights of data subjects²⁵ by F. Rossi Dal Pozzo²⁶, P. Hobbing²⁷, D. Louks²⁸. However, 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements have never been analyzed in comparative perspective by scholars.

A valuable contribution to the interpretation and understanding of the compatibility of the provisions of the PNR Agreements with EU primary law is brought by the case law of CJEU and ECtHR, in particular, Opinion of the Advocate General²⁹, as well as, opinions of the relevant institutions involved in the process of implementation, review and enforcement of PNR Agreements. Furthermore, 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements have never been analyzed in comparative perspective taking into account PNR agreements which have already expired.

However, until recently none of the PNR Agreements has been assessed by the CJEU in the light of EU primary law, in particular, the the Charter of Fundamental Rights of the EU (hereinafter Charter). This is also the first time that the Court is required to rule on the compatibility of the 2014 EU-Canada draft PNR agreement with the fundamental rights enshrined in the Charter and more particularly with those relating to respect for private and family life, guaranteed by Article 7, and the protection of personal data, guaranteed by Article 8. Even though the 2004 EU-USA PNR Agreement³⁰ was brought before CJEU³¹ the Court focused its attention on purely procedural aspects, such as those concerning the scope of Directive 95/46 and the Community competence to conclude an agreement in a specific area under Article 95 TCE.³²

Therefore, the thesis focuses on the comprehensive and combine analyzes of the PNR Agreements and their compatibility with EU primary law in a comparative perspective.

²⁵ Rossi Dal Pozzo, F. "EU Legal Framework for Safeguarding Air Passenger Rights", supra note 21, see also Hobbing, P. "Tracking Terrorists: The EU-Canada Agreement in PNR Matters", supra note 6 and Louks D., "(Fly) Anywhere but here: approaching US-US dialogue concerning PNR in the era of Lisbon", supra note 17.

²⁶ F. Rossi Dal Pozzo "EU Legal Framework for Safeguarding Air Passenger Rights", *ibid.*, p. 119

²⁷ Hobbing, P., *op. cit.*, p. 10.

²⁸ Douglas Louks, *op. cit.*

²⁹ Opinion 1/15, supra note 14.

³⁰ 2004 EU-USA PNR Agreement, supra note 8.

³¹ Joined Cases C-317/04 and C-318/04, European Parliament. Council of the European Union, PNR, [2006] ECR I-04721.

³² Nino, M., "The protection of personal data in the fight against terrorism", supra note 20, p. 73.

Significance of the thesis. The research undertaken by the thesis has theoretical and practical significance. While thesis focuses on the comprehensive and combine analyzes of the PNR Agreements and their compatibility with EU primary law in a comparative perspective it may give added value to the future researches, conferences and lectures or may be helpful studying training material for students specializing in criminal or human rights law.

The aim and the objectives of the thesis. The aim of the thesis is to determine legality of the 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements in the light of EU primary law.

For the purpose of this aim, the following objectives are discerned:

- 1) To examine historical events in order to perceive the circumstances that led to the conclusion of EU-Canada, EU-USA and EU-Australia PNR Agreements.
- 2) To examine the notions of PNR and API data, their substantial difference;
- 3) To identify which human rights standards are applicable while evaluating EU PNR Agreements and disclose their content;
- 4) Relying on the existing legal framework, doctrine provided by the scholars, case law of the CJEU and particularly, Opinion of the Advocate General of the CJEU on compatibility of the 2014 EU-Canada PNR Agreement regarding rights guaranteed by the Charter in particular the rights to privacy and data protection, to ascertain necessity and proportionality of the PNR Agreements' provisions regarding period of data retention, data processing, data elements to be collected, disclosure of data to other government authorities and third countries and guarantees for and rights of data subjects.

The methodology of the thesis. To achieve the objective of the research, the thesis employed the following methods:

- 1) systematic analysis method – was used to examine the content and scope of API and PNR data, to identify which human rights standards taking into account the hierarchy of EU norms should be applicable while evaluating EU PNR agreements, as well as to examine the content and scope of privacy and data protection including application of

those guarantees in the case law of CJEU and ECtHR, to examine the content and scope of the procedure of revision of the PNR Agreements and certain provisions of Agreements themselves, to show the problematic or unclear aspects of PNR Agreements.

- 2) comparative method – was used to compare API and PNR data, the historical and contemporary provisions of PNR Agreements and to compare contemporary provisions of currently applicable PNR Agreements among each other, Charter and Convention provisions applicable for privacy and data protection as well as CJEU and ECtHR practices towards privacy and data protection, likewise to identify their similarities and differences.
- 3) documentary analysis – was used to analyse EU and international documents, their provisions, case-law of CJEU and ECtHR.
- 4) resumptive method – was used to resume opinions presented by EU and Canada, USA, Australia institutions, judicial practice and academic opinions. The method was also employed for making the conclusions.
- 5) linguistic method was used to ascertain the content of the provisions of EU and international documents, in particular, PNR agreements relying on their formulation. The method was used together with teleological method when interpreting the content of the provisions, relying on the purpose of certain provisions.

The structure of the thesis. The thesis is constructed as a comparison of theory and practice: examination of the legal theory of the right to privacy and data protection and the analysis of the particular PNR Agreements concluded by EU with Canada, USA and Australia. Generally, thesis consists of introduction, three chapters, conclusions and proposals.

Thus, in order to achieve the above-mentioned objectives, thesis consists of three main parts. The first part provides the analysis of the concepts of API and PNR data: their definitions, substantial differences and legal documents, which regulate the use of them. It also examines certain historical events and the aftermath of it, which led to the conclusion of first PNR Agreements with Canada, USA and Australia. The second part identifies, first of all, which human rights standards taking into

account the hierarchy of EU norms should be applicable while evaluating EU PNR agreements. Then it focuses on the origins of EU data protection law and the distinction between “privacy” and “data protection”, as well the content of the rights relevant to further evaluation of PNR agreements. Finally, the Chapter describes and analyses the assessment of the effectiveness of the procedure, which is applied for the revision of the EU PNR agreements, in case any infringements or inconsistencies are detected. The third part of the thesis focuses on the assessment of the particular provisions of the PNR Agreements concluded EU with Canada, USA and Australia: historical development of the provisions and current forms provided in the most recently concluded PNR Agreements. In the light of Articles 7, 8 and 52(1) of the Charter this part focuses on the necessity to conclude PNR Agreements in the first place and proportionality of mostly criticized provisions such as rather long period of data retention, wide spectrum of data processing purposes, a large amount of data elements to be collected, disclosure of data to other government authorities and third countries and guarantees for and rights of data subjects.

Statement to defend:

2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements are incompatible with the fundamental rights enshrined in the Charter relating to respect for private and family life, guaranteed by Article 7, and the protection of personal data, guaranteed by Article 8, therefore are illegal.

I. GENERAL CONCEPTS AND THE NEED FOR EU BILATERAL PNR AGREEMENTS

The technological developments in the society can be used as a tool to deal with the global, constantly growing crime rates. Among such tools are Advance Passenger Information (hereinafter API) and Passenger Name Record (hereinafter PNR) data. However, API data are different and more limited in scope and should not be confused with Passenger Name Record (PNR) data. Therefore, the following Chapter provides the analysis of the concepts of API and PNR data: their definitions and substantial differences and legal documents which regulate the use of them. Meanwhile, after 9/11 attacks in USA PNR data have been identified as invaluable tool for investigating and precluding terrorist attacks. Thus, a number of non-EU countries started to require air carriers arriving at their territory to submit PNR data. USA, Canada and Australia were among those countries. Therefore, EU was in need to conclude bilateral PNR Agreements.

1.1. Concept of API and PNR data

API data involves “the capture of a passenger's biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country”³³. In other words, API data are basically the biographical information taken from the machine-readable part of a passport and contain the name, place of birth and nationality of the person, the passport number and expiry date.³⁴ Moreover, it includes some other itinerary details such as destination address, place of original embarkation, place of clearance, place of onward foreign destination, destination address.³⁵

In the EU, the API Directive regulates the use of API data³⁶. According to the Directive, API data should be made available to border control authorities, at the request of each Member State, for flights entering the territory of the EU for the purpose of improving border controls and combating

³³ WCO/IATA/ICAO “Guidelines on Advance Passenger Information (API)”, 2010, pp. 3.8.

³⁴ 2014 EU-Canada PNR Agreement, *supra* note 12, p. 7.

³⁵ WCO/IATA/ICAO “Guidelines on Advance Passenger Information (API)”, 2010, pp.7.1.5., see also Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data OJ L 261, 6.8.2004, p. 24–27. pp. 3(2) (the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, the initial point of embarkation).

³⁶ Council Directive 2004/82/EC, *op. cit.*

irregular immigration.³⁷ Even though Directive provides API data for law enforcement purposes, this is possible only if specific criteria are fulfilled.³⁸ Thus, albeit API data are in some cases used by law enforcement authorities in order to identify suspects and persons sought, they are mainly used as identity verification.³⁹ Furthermore, API data do not enable law enforcement authorities to conduct a profile-based assessment of passengers, and therefore do not facilitate the detection of hitherto ‘unknown’ criminals.⁴⁰ In fact, API data are different and more limited in scope and should not be confused with PNR data.

PNR, in the air transport industry, “is the generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger”⁴¹. PNR data is unverified information provided by passengers, and collected by and held in the carriers’ reservation and departure control systems for their own commercial and operational purposes in providing air transportation services.⁴² PNR data involves several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent at which the flight was booked, means of payment used, seat number and baggage information.⁴³ In other words, PNR data may contain as little information as a name, an itinerary, some generic contact information and a ticketing/ticketed indicator.⁴⁴ However, sometimes PNRs contain vast amounts of information covering a wide range of issues relating to the person’s special service requests, contact details, credit card information and other data.⁴⁵

In nowadays environment, carriers are often limited in what data contained in passenger reservations (PNRs) can be shared with requesting authorities.⁴⁶ Furthermore, certain data are considered particularly sensitive and may not be shared in accordance with many States’ data privacy legislation.⁴⁷ While PNR data can be used to identify a person, it may be used for customs, law

³⁷ Council Directive 2004/82/EC, *supra* note 35, pp. 1, 3(1).

³⁸ Council Directive 2004/82/EC, *ibid.*, pp. 6(1)

³⁹ Proposal for a Directive on the use of Passenger Name Record data, *supra* note 2, p. 7.

⁴⁰ *Ibid.*, p. 7.

⁴¹ International Civil Aviation Organization “Guidelines on Passenger Name Record (PNR) data”, Approved by the Secretary General and published under his authority, First Edition — 2010, pp. 2.1.1.

⁴² *Ibid.*, pp. 2.1.1, see also Proposal for a Directive on the use of Passenger Name Record data, *supra* note 2, p.3

⁴³ Proposal for a Directive on the use of Passenger Name Record data, *supra* note 2, p.3

⁴⁴ International Air Transportation Association (IATA), Passenger Data Exchange: The Basics, <<http://www.iata.org/iata/passenger-data-toolkit/presentation.html>> [accessed 11.17.2016], p. 13.

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

enforcement purposes, security and more importantly risk-based assessment of persons about whom one may not have collected any information, and is typically more valuable in the identification of suspicious trends, relationships and travel patterns.⁴⁸ Furthermore, law enforcement authorities may use PNR data in several ways such as 1) *re-active*: using data for investigations, prosecutions, unravelling of networks after a crime has been committed; 2) *real-time*: using PNR data prior to the arrival or departure of passengers in order to prevent crime, take other necessary actions before a crime has been committed or because a crime has been or is being committed, in this manner PNR data functions as a tool of assessing passenger risks and identifying “unknown” and/or “high risk” persons; and (3) *pro-active*: using data for analysing and creating assessment criteria, which can be used later for a pre-arrival and pre-departure assessment of passengers.⁴⁹ Until recently, the use of PNR data has not been regulated at EU level. There were only couple of Member States that developed their own PNR systems (e.g. UK, France). It will change with the currently adopted PNR Directive⁵⁰, which will be discussed in Chapter 1.3.

In a nutshell, API data is limited in scope, different from and should not be confused with PNR data. API data does not enable law enforcement authorities to conduct an assessment of passengers against targeting rules, and therefore does not facilitate the detection of hitherto ‘unknown’ criminals. Even though API data can be used by law enforcement authorities in order to identify suspects and persons sought, they are mainly used as identity verification and border management tool. Whilst, PNR data can be used to identify a person, but it might be used for customs, law enforcement purposes, security and more importantly risk-based assessment of persons about whom one may not have collected any information, and is typically more valuable in the identification of suspicious trends, relationships and travel patterns.

1.2.The need for EU bilateral PNR Agreements with non-EU countries

⁴⁸ International Air Transportation Association (IATA), Passenger Data Exchange, supra note 44, p. 9.

⁴⁹ Proposal for Directive on the use of passenger name record (PNR) data, supra note 2, p. 3,4.

⁵⁰ Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

On 11 September 2001 the United States became a transformed nation.⁵¹ Terrorists boarded four planes and headed to the east coast of the United States. Once in control, these terrorists-pilots took their aim for an attack at the heart of the American financial, governmental and defense centres.⁵² Three aircrafts hit their targets, successfully crashing, into both World Trade Centres (The Twin Towers) located in the New York City and the Pentagon in Washington D.C. while the fourth, presumably aimed at one of the following the Capitol Building or the White House in Washington D.C., crashed in a field in Pennsylvania.⁵³

Moreover, the Madrid train bombing on 11 March 2004 “not only demonstrated vulnerabilities of European rail transportation system: they also highlighted weaknesses in European border security”⁵⁴. An al-Qaeda-affiliated group linked to bombing in Madrid, Ansar al-Islam, had document fraud operations and human smuggling to fund terrorist actions and smuggle its own members into Spain and Iraq. Some of the al-Qaeda members who planned and executed the 9/11 plot lived and were recruited in Europe. It was clear that European immigration and border control policies are crucial to US homeland security.⁵⁵

These events revealed a long list of security weaknesses in global transportation and border control systems⁵⁶, especially with regard to the supervision/enforcement of visa and passport requirements⁵⁷. Pinpointing loopholes in pre-9/11 border control systems, the United States government concluded that PNR data were invaluable tools for investigating and precluding terrorist attacks.⁵⁸

After 9/11 events, in the context of the fight against international terrorism, the EU has concluded Agreements with third countries, such as the United States, Canada and Australia, aimed at

⁵¹ The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary, p. 1.

⁵² Louks, D., “(Fly) Anywhere but here: approaching US-US dialogue concerning PNR in the era of Lisbon”, supra note 17, p. 479.

⁵³ Ibid., p. 479.

⁵⁴ Kozłowski, R. Border and Transportation Security in the Transatlantic Relationship”, supra note 18, pp. 89–105, p. 80.

⁵⁵ Ibid., p. 80.

⁵⁶ Ibid., p. 80.

⁵⁷ Hobbing, p. “Tracking Terrorists: The EU-Canada Agreement in PNR Matters”, supra note 19, p. 10.

⁵⁸ Ibid, p. 10.

transferring and processing air passengers' personal data.⁵⁹ Reasoning of the need for bilateral PNR Agreements concluded between EU and previously mentioned countries is the following.

Just a few months after the 9/11 attacks, on 19 November 2001, the US adopted a new Aviation and Transportation Security Act (hereinafter ATSA), which required all airlines with US-bound international flights to submit a passenger manifest, concerning the information of all aboard, electronically to the Customs and Border Protection systems.⁶⁰ Manifests' information included, full name, date of birth and citizenship, gender, passport number and country of issuance, the US visa number or resident alien card number.⁶¹ For those airlines, which failed to comply and transmit this information before or soon after either heavy fines could be imposed or even the landing of their planes on the American soil could be denied.⁶² The entire transatlantic negotiation round started in 2002 to develop conditions for an arrangement dealing with the transmission of the required passenger information⁶³ as an emergency measure when European airlines were confronted with the urgent choice of either facing heavy fines/loss of the US landing rights (when not complying with the new US PNR rules) or infringing EU data protection laws⁶⁴ as laid down in Directive 95/46/EC⁶⁵. Eventually, the EU and the US agreed to terms on the Passenger Name Record (PNR) Agreement signed in 2004.⁶⁶ Following this very first EU-USA PNR Agreement, three more EU-USA PNR Agreements were signed. The 2006 EU-USA Interim PNR Agreement⁶⁷ replaced the 2004 Agreement which was annulled by Court of Justice of the EU (hereinafter CJEU) for the lack of the Community competence to conclude an agreement in a specific area under Article 95 TCE.⁶⁸

⁵⁹ Nino, M., "The protection of personal data in the fight against terrorism", supra note 20, p. 62.

⁶⁰ Louks, D., "(Fly) Anywhere but here: approaching US-US dialogue concerning PNR in the era of Lisbon", supra note 17, p. 480

⁶¹ 49 USC 44939 note, Aviation and Transportation Security Act (ATSA), Public Law 107-71, November 19, 2001, SEC. 115. PASSENGER MANIFESTS, pp. 2. Also see 2(f) Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety.

⁶² Louks, D., op. cit., p. 480.

⁶³ Louks, D., ibid, p. 480.

⁶⁴ Hobbing, P. "Tracing Terrorists: The EU-Canada Agreement in PNR Matters", supra note 19, p. 10

⁶⁵ Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004.

⁶⁶ 2004 EU-USA PNR Agreement, supra note 8.

⁶⁷ 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, OJL 298, 27.10.2006. [hereinafter 2006 EU-USA Interim PNR Agreement].

⁶⁸ Nino, M., "The protection of personal data in the fight against terrorism", supra note 20, p. 73

The new definitive EU-PNR Agreement went into force in 2007⁶⁹. The current Agreement was signed and went into force in 2012 and is still in effect until now.⁷⁰

The internal Canadian requirement for airlines to provide API/PNR data had been adopted by the new Public Safety Act of 22 November 2001.⁷¹ Even though, there had been no formal treaty commitment or request by the US, it was noticeable from the overall scenario that Canada took this action as part of its post-9/11 solidarity and to be in compliance with the general standards set by the ‘senior partner’, according to a traditional pattern in US–Canadian relations.⁷² In accordance with their domestic legislation, since January 2003 US Customs⁷³ and later the Canada Border Services Agency⁷⁴ (hereinafter CBSA) has required Europe-based airlines to submit information on US-bound air passengers.⁷⁵ As a matter of fact, API/PNR system was set up in Canada in 2002 with the collection of API data beginning on 7 October 2002 and PNR data on 8 July 2003.⁷⁶

While some of the companies immediately complied with the request – even allowing US Customs to collect the relevant data directly from the airline databases, others refused on the grounds that the transfer would violate EU data protection provisions.⁷⁷ Essentially, “European airlines were presented with the choice of either breaking US laws or facing fines and potentially losing landing rights, or violating EU data protection laws and facing fines”⁷⁸. Accustomed to the situation from experience with the US, the EU reacted swiftly and entered into negotiations⁷⁹ that led to the EU–Canada Agreement in API/PNR matters of 2006⁸⁰. Following negotiations the new PNR Agreement was initialed on 6 May 2013.⁸¹ The EU and Canada signed their new agreement on the processing

⁶⁹ 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), OJL 204,4.8.2007, [hereinafter 2007 EU-USA PNR Agreement].

⁷⁰ 2012 EU-USA PNR Agreement.

⁷¹ Public Safety Act, 2002 (S.C. 2004, c. 15).

⁷² Hobbing, P., “Tracking Terrorists: The EU-Canada Agreement in PNR Matters”, supra note 19, p. 7.

⁷³ This is based on the US Aviation and Transportation Security Act of 19 November 2001 and the Enhanced Border Security and Visa Entry Reform Act of 14 May 2002 (EPIC, 2007).

⁷⁴ This is based on section 107.1 of the Customs Act (Bill C-17).

⁷⁵ Guild, E. and Brouwer, E., “The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US”, CEPS Policy Brief No. 109, CEPS, Brussels, 26 July, 2006.

⁷⁶ Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines, WP 88, 11 February, Brussels, pp. 5

⁷⁷ Hobbing, P., “Tracking Terrorists: The EU-Canada Agreement in PNR Matters”, supra note 19, p. 7.

⁷⁸ Kozłowski, R. “Border and Transportation Security in the Transatlantic Relationship, supra note 18, p. 85

⁷⁹ Hobbing, P., op. cit., p. 7

⁸⁰ 2006 EU-Canada PNR Agreement, supra note 9.

⁸¹ Rossi Dal Pozzo, F. “EU Legal Framework for Safeguarding Air Passenger Rights”, supra note 21 , p. 119

and transfer of Passenger Name Record (PNR) data by air carriers to the Canadian competent authorities on 25 June 2014.⁸² However, in November 2014, following the decision of the CJEU in Data Retention Directive case⁸³, EU Parliament brought a case before the CJEU to assess the compatibility of the 2014 PNR Agreement regarding rights guaranteed under EU treaties, in particular the rights to privacy and data protection⁸⁴. As of 31 December 2016 the case is still pending in Court. On 8 September 2016, Paolo Mengozzi, Advocate General of the CJEU, who has been assigned to this case, released his Opinion⁸⁵, which will be discussed in section 3. In fact, a previous 2006 EU-Canada PNR Agreement remains in force until a new one can replace it.

On 28 February 2008, the Council assisted by the Commission decided to open negotiations for an Agreement between the EU and Australia on the processing and transfer of EU-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service (hereinafter ACS).⁸⁶ Those negotiations were successful and a draft Agreement was drawn up, which was signed by the EU with Council Decision 2008/651/CFSP/JHA of 30 June 2008.⁸⁷

This was the first sign of a broader cooperation between Australia and EU⁸⁸. First of all, this PNR Agreement was necessary “[...] for facilitating passenger arrival clearances and for border security at airports in Australia” and most importantly, because the Australian national airlines – Qantas “[...] moved its PNR information management system to Germany”⁸⁹. However, European Parliament expressed its critical evaluation of 2008 EU-Australia PNR Agreement in its Recommendation of 2008⁹⁰. In this evaluation it observed that the procedure followed by the

⁸² Council of the EU, Signature of the EU-Canada agreement on Passenger Name Records (PNR), Brussels, 25 June 2014, 10940/14, PRESSE 339, <

[http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-\(pnr\)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-a](http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-a) [last accessed 12-27-2016].

⁸³ Joined Cases C-293/12 and C-594/12 [2014], ECLI:EU:C:2014:238.

⁸⁴ Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU, Opinion 1/15, 2015/C 138/32.

⁸⁵ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29.

⁸⁶ Rossi Dal Pozzo, F, *op. cit.*, p. 114

⁸⁷ 2008 EU-Australia PNR Agreement, *supra* note 10.

⁸⁸ Kaunert, C., Leonard, S. and Pawlak, P., *supra* note 22, p. 103

⁸⁹ Joint Media release with Minister for Home Affairs, The Hon Bob Debus MP 1 July 2008 on Australia and the EU Sign Passenger Name Record (PNR) Agreement, <http://foreignminister.gov.au/releases/2008/fa-s080701.html> [last accessed 10/20/2016].

⁹⁰ European Parliament recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the EU and Australia on the processing and transfer of EU sourced passenger name record (PNR) data by air carriers to the Australian customs service (2008/2187(INI)), OJEU C 15E, 21.1.2010, p. 46.

Council completely lacked democratic legitimacy since the European Parliament had not been informed on the adoption of the mandate, the conduct of the negotiations or the conclusion of the Agreement.⁹¹ Furthermore, it also expressed its concern as to the legal basis for the Agreement, since the latter focused almost entirely on the internal security needs of a third State and thus did not bring any added benefits to EU Member States or their citizens⁹². This led to the postponement of the conclusion of the Agreement, however it being applicable on the provisional basis from the date of its signature.⁹³

With the entry into force of the Treaty of Lisbon the EU needed to amend the Agreement.⁹⁴ The European Parliament called for a review of the Agreement by 30 June 2010, however, with Resolution of 5 May 2010⁹⁵ European Parliament, in view of its previous criticism, declared its intention of postponing the vote on the request for consent to the 2008 Agreements with Australia until the modalities regarding the use of PNR were brought into line with EU law.⁹⁶ European Parliament with its new Resolution of 11 November 2010⁹⁷ yet again underlined the importance of opening negotiations with Australia for new international agreement on the transfer and processing of PNR. The new negotiation phase ended on 22 September 2011, when the Council, with Decision 2012/380/EU⁹⁸ authorized the signing of the new PNR Agreement on behalf of the EU⁹⁹ and it was successfully voted by the European Parliament on 27 October 2011¹⁰⁰. The new EU-Australia PNR Agreement¹⁰¹ entered into force on 1 June 2012 and is still valid. It replaced the 2008 PNR Agreement between EU and Australia.

⁹¹ Rossi Dal Pozzo, F., “EU Legal Framework for Safeguarding Air Passenger Rights”, 21, p. 115

⁹² Ibid., p. 115

⁹³ Ibid., p. 115

⁹⁴ Blasi Casagran, C., “Global Data Protection in the Field of Law Enforcement– An EU Perspective”, supra note 23, p. 110

⁹⁵ European Parliament Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, OJEU C 81E, 15.3.2011, p. 70.

⁹⁶ Rossi Dal Pozzo, F., op. cit., p. 114

⁹⁷ European Parliament Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the EU and Australia, Canada and the United States, OJEU C 74E, 13.3.2012, p. 8.

⁹⁸ 2012 EU-Australia PNR Agreement, supra note 11, p. 2.

⁹⁹ Rossi Dal Pozzo, F. op. cit., p. 116.

¹⁰⁰ Blasi Casagran, C., “ Global Data Protection in the Field of Law Enforcement– An EU Perspective”, supra note 23, 2017, p. 110

¹⁰¹ 2012 EU-Australia PNR Agreement, supra note 11, p. 4.

On 14 July 2015, negotiations for an EU-Mexico PNR data transfer deal were formally commenced.¹⁰² Unfortunately, negotiation documents are not publicly accessible; therefore this PNR Agreement is not an object of this research.

To sum up, the EU was in need to conclude bilateral PNR Agreements with US as an emergency measure when European airlines were confronted with the urgent need to comply with the new US PNR rules. Furthermore, when Canada adopted its national laws concerning PNR rules, accustomed to the situation from experience with the US, the EU reacted swiftly and went into PNR agreements with Canada as well. EU-Australia PNR Agreements were further evidence of US influence, which opened the door for other states to make PNR Agreements with the EU.

1.3. EU PNR directive

As it was mentioned above, until 2016, the use of PNR data was not regulated at EU level, even though several Member States have developed their own PNR systems. Even to date, only a limited number of Member States set up a PNR system, most Member States had used PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime in a non-systematic way or under general powers granted to the police or other authorities¹⁰³ For instance, intelligent and law enforcement agencies could require to access PNR data via a court order, following the regular procedures prescribed by law.¹⁰⁴ In 2011, when the EU PNR Directive was proposed by the Commission only the United Kingdom had fully-fledged PNR data collection system, while France, Denmark, Belgium, Sweden and the Netherlands had either enacted relevant legislation or were currently testing using PNR data.¹⁰⁵ Several other Member States were considering setting up PNR.¹⁰⁶ As a result, up to 27 considerably diverging systems could have been created resulting in uneven levels of protection of personal data across the EU, security gaps, increased costs and legal uncertainty for air carriers and passengers alike.¹⁰⁷

¹⁰² European Parliament, “EU Passenger Name Record (PNR) directive: an overview”, Justice and home affairs, 01-06-2016, <[http://www.europarl.europa.eu/news/lt/news-room/20150123BKG12902/eu-passenger-name-record-\(pnr\)-directive-an-overview](http://www.europarl.europa.eu/news/lt/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview)> [last accessed 11-20-2016].

¹⁰³ Proposal for a directive on the use of PNR data, supra note 2, p. 4.

¹⁰⁴ European Digital Rights (EDRi) by Diego Naranjo, FAQ: Passenger Name Records (PNR), 09 Dec 2015, <https://edri.org/faq-pnr/>, [last accessed 12-5-2016]

¹⁰⁵ Proposal for a Directive on the use of PNR data, op. cit., p. 4.

¹⁰⁶ Proposal for a Directive on the use of PNR data, ibid, p. 4.

¹⁰⁷ Proposal for a Directive on the use of PNR data, supra note 2, p. 4.

To prevent this from happening, the EU took matters into its own control and in April 2016 adopted PNR Directive aiming to harmonize Member States' provisions on obligations for air carriers to transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.¹⁰⁸ Furthermore, before the adoption of EU PNR Directive third countries did not give the PNR data to the EU, because Agreements provided for a unilateral transfer of PNR data.¹⁰⁹ This PNR Directive was published in the Official Journal of the EU on 27 April 2016, from that moment according to the EU law Member States will have an obligation to transpose the legislation into their national laws in two years period.

PNR Directive aims to regulate processing of PNR data transferred from the airlines to national authorities in Member States.¹¹⁰ Under this Directive, airlines will be obliged to provide PNR data for flights between EU and third countries, that is to say, flights from third country entering into any Member States or departing from the EU into any third country.¹¹¹ It will also allow, but not oblige, Member States to collect PNR data concerning selected intra-EU flights.¹¹² The Directive establishes that collected PNR data may only be processed including its collection, use and retention by Member States and its exchange between Member States for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.¹¹³ Air carriers will transfer collected PNR by the so-called “push”¹¹⁴ method, meaning that Member States will not have direct access to the carriers' IT systems.¹¹⁵

Under PNR Directive “each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its Passenger Information Unit (hereinafter PIU)”¹¹⁶. PNR data will be sent by air carriers to PIU of the Member State in which the international flight arrives or

¹⁰⁸ Ibid, p. 4.

¹⁰⁹ 2006 EU-Canada PNR Agreement, *supra* note 9, pp. 1.

¹¹⁰ Directive (EU) 2016/681 on the use of passenger name record (PNR) data, *supra* note 50, pp. 1(a, b).

¹¹¹ Ibid., pp. 1(a), 3(2).

¹¹² Ibid., pp. 2.

¹¹³ Ibid., pp. 1(b, c).

¹¹⁴ “push” method is a method under which air carriers transfer (‘push’) the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided.

¹¹⁵ Directive (EU) 2016/681 on the use of passenger name record (PNR) data, *op. cit.*, pp. 8

¹¹⁶ Directive (EU) 2016/681 on the use of passenger name record (PNR) data, *supra* note 50, pp. 4(1).

from which it departs.¹¹⁷ The PIU would be responsible for “collecting PNR data, storing them, processing those data, transferring those data or the results of processing them to the competent authorities [...]”¹¹⁸ and exchanging of the received information with the PIUs of other Member States and with Europol¹¹⁹. Transfer of PIU stored PNR data to third countries can only take place in very limited circumstances and on a case-by-case basis.¹²⁰ An independent national supervisory authority shall be provided by each Member State and shall be responsible for advising and monitoring the application of the provisions adopted pursuant to PNR Directive.¹²¹

The Directive provides a list of 19 PNR elements to be collected and prohibits the collection and use of sensitive data.¹²² Under PNR Directive PNR data can only be kept for a period of 5 years, and must be depersonalised after a period of 6 months so the data subject is no longer immediately identifiable and must be deleted permanently upon the expiry of 5 years period.¹²³ According to the PNR Directive, Member States shall ensure that passengers are clearly informed about the collection of PNR data and of their rights.¹²⁴

To sum up, EU PNR Directive was adopted to harmonize Member States’ provisions on obligations for air carriers to transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. EU PNR Agreements concluded with third countries were not enough to regulate this area because Agreements provided unilateral PNR data transmission. PNR Directive it is without prejudice to bilateral agreements concluded with third countries. Furthermore, PNR Directive has lower hierarchy in hierarchy of norms in EU and is valid only if it is compatible with the international acts and agreements, which have precedence over it.

¹¹⁷ European Parliament, “EU Passenger Name Record (PNR) directive: an overview”, supra note 102.

¹¹⁸ Directive (EU) 2016/681 on the use of passenger name record (PNR) data, op. cit., pp. 4(2a). Each member state would have to approve a list of the competent authorities entitled to request or receive PNR data or the result of the processing of PNR data from the PIU (pp.8)

¹¹⁹ Ibid., pp. 4(2b).

¹²⁰ Ibid., pp. 1.

¹²¹ Ibid., pp. 15(1).

¹²² Ibid., pp. 15(1), pp. 13(4), ANNEX I Passenger name record data as far as collected by air carriers.

¹²³ Ibid., pp. 12 (1,2)

¹²⁴ Ibid., pp. 13, Whereas (28).

II. FUNDAMENTAL HUMAN RIGHTS STANDARDS APPLICABLE FOR THE ASSESSMENT OF PNR AGREEMENTS

EU PNR Agreements concluded with US, Australia and Canada were criticized many times by European Data protection agency - European Digital Rights¹²⁵ as well as European Parliament¹²⁶, European Commission¹²⁷, the Article 29 Data Protection Working Party (hereinafter Art. 29WP)¹²⁸ and scholars¹²⁹ for over-stepping a fair balance between the legitimate desire to preserve public security and the equally fundamental right for everyone to be able to enjoy a high level of protection of his private life and his own personal data.¹³⁰ In particular, considerable amount of criticism was directed to rather long period of data retention, wide spectrum of data processing purposes, a large amount of data elements to be collected, disclosure of data to other government authorities and third countries and guarantees for and rights of data subjects.

In the light of aforementioned criticism, the following Chapter identifies, first of all, which human rights standards taking into account the hierarchy of EU norms should be applicable while evaluating EU PNR agreements. Then it focuses on the origins of EU data protection law and the distinction between “privacy” and “data protection”, as well the content of the rights relevant to further evaluation of PNR agreements. Finally, the Chapter deals with the assessment of the effectiveness of the procedure, which is applied for the revision of the EU PNR agreements, in case any infringements or inconsistencies are detected.

¹²⁵ European Digital Rights, <https://edri.org/theme/privacy/> [last accessed 12-06-2012]

¹²⁶ European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144.

¹²⁷ Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM (2010) 492 final, 21.9.2010.

¹²⁸ Article 29 Data Protection Working Party, and to the letter of 6 January 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf [last accessed 12-06-2016] see also The Article 29 Working Party (Art. 29 WP) is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The composition and purpose of Art. 29 WP was set out in Article 29 of the Data Protection Directive, and it was launched in 1996. It is a very important platform for cooperation, and its main tasks are to: Provide expert advice from the national level to the European Commission on data protection matters; Promote the uniform application of Directive 95/46 in all Member States of the EU, as well as in Norway, Liechtenstein and Iceland; Advise the Commission on any European Community law (so called first pillar), that affects the right to protection of personal data).

¹²⁹ Rossi Dal Pozzo, F., “EU Legal Framework for Safeguarding Air Passenger Rights”, supra note 21, see also Hobbing, P., “Tracking Terrorists: The EU-Canada Agreement in PNR Matters”, supra note 19, Louks, D., “(Fly) Anywhere but here: approaching EU-USA dialogue concerning PNR in the era of Lisbon”, supra note 17.

¹³⁰ Opinion of Advocate General Kokott delivered on 6 October 2011 Case C-366/10 Air Transport Association of America and Others, ECLI:EU:C:2011:637, pp. 8.

2.1. Data protection regulations ascertained in the EU

In a hierarchy of norms in EU law, international agreements concluded by the EU are subordinate to primary legislation therefore they cannot contradict primary law.¹³¹ In conformity with the principles of international law, EU institutions, having power to negotiate and conclude an international agreement are free to agree with the third States concerned what effect the provisions of the agreement are to have in the internal legal order of the contracting parties. Only if that question has not been settled by the agreement it falls to be decided by the Courts having jurisdiction in the matter, and in particular by the CJEU, in the same manner as any question of interpretation relating to the application of the agreement in the EU.¹³²

For a very long period of time, in the EU collecting, processing, retention and transferring of personal data was regulated by the Directive 95/46/EC¹³³ which attempted to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States (commonly referred to as the EU Data Protection Directive). The EU Data Protection Directive was considered to be the central pillar of data protection in the EU.¹³⁴ However, the exception enshrined in the Directive as regards data processing for public security and criminal law enforcement purposes was applied by the CJEU in a major case concerning the transfer of PNR data to the US for the purpose of preventing and combating terrorism and border protection following the terrorist attacks on 11 September 2001.¹³⁵ The decision on adequacy involved the processing of personal data not falling within the scope of Directive 95/46 and, as a consequence, it infringed the Community norm itself. Therefore, CJEU stated that the decisions adopted by Community on adequacy of Agreement involved the processing of personal data not falling within the scope of Directive 95/46 and, as a consequence, it infringed

¹³¹ European Parliament, “Sources and scope of EU law”, Fact Sheets on the EU, Udo Bux, 10/2016, p. 1, http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf [last accessed 12-27-2016].

¹³² Case-366/10 - Air Transport Association of America and Others [2011] ECR I-13755, pp. 49

¹³³ 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, supra note 35.

¹³⁴ Milon Gupta, Privacy and Data Protection in the EU in Eurescom message, issue 3/2011 (2011); <http://www.eurescom.eu/fileadmin/documents/message/EURESCOM_message_03-2011.pdf> [last accessed 11.24.2016].

¹³⁵ Joined Cases C-317/04 and C-318/04, European Parliament. Council of the European Union, PNR, [2006] ECR I-04721.

the Community norm itself.¹³⁶ In other words, the Data Protection Directive did not apply to the processing of personal data stipulated under PNR Agreements.

The Data Protection Directive will be repealed by Regulation (EU) 2016/679¹³⁷ of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter General Data Protection Regulation). General Data Protection Regulation will come into force on 25 May 2018. This step was basically taken because the EU Data Protection Directive resembled a patchwork of slightly different laws across Europe. The objective of this Regulation is to contribute better to the “[...] accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons”¹³⁸. It is very important to notice that, EU PNR Directive and EU Data Protection Regulation were adopted almost at the same day. The European Commission stated that the objective of this new set of rules was to give citizens back control over of their personal data, and to simplify the regulatory environment for business.¹³⁹ However, the material scope of the EU Data Protection Regulation closely resembles the scope of the current EU Data Protection Directive: it applies to all processing of personal data wholly or partly by automated means, and to the processing by other means of personal data in or intended for a filing system, except in a few situations which in substance correspond with those mentioned in the Directive.¹⁴⁰ Therefore, Regulation does not apply to the processing of personal data in any case concerning public security, defence and State security that is to say for law enforcement purposes.¹⁴¹ Thus, it does not apply to the PNR Agreements concluded by EU with US, Canada and Australia.

¹³⁶ Ibid, pp. 59-60.

¹³⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [hereinafter General Data Protection Regulation], OJ L 119, 4.5.2016, p. 1–88.

¹³⁸ General Data Protection Regulation, op. cit., Whereas 2,3.

¹³⁹ European Commission official webpage “Protection of personal data”, < <http://ec.europa.eu/justice/data-protection/>> [last accessed 12-08-2016]

¹⁴⁰ Hustinx, P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", p. 29.

¹⁴¹ General Data Protection Regulation, supra note 137, pp. 2(2).

EU has adopted Directive 2016/680¹⁴² on 27 April 2016 concerning particularly the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. However, it does not again apply to the PNR Agreements concluded by EU with US, Canada and Australia.

Notwithstanding that, while assessing PNR Agreements under Article 218(11) the Treaty on the Functioning of the EU¹⁴³ (hereinafter the TFEU), the only provisions by reference to which the compatibility of the international agreements may be examined are the provisions of EU primary law, that is to say, the Treaties and the rights set out in the Charter, to the exclusion of secondary law.¹⁴⁴

To sum up, although EU has adopted Regulations and Directives on the processing of personal data these instruments cannot be applicable while assessing legality of international agreements, to be exact, PNR Agreements concluded by EU with USA, Canada and Australia. EU secondary legislation is the next level down in the hierarchy and is valid only if it is consistent with the acts and agreements, which have precedence over it. Therefore, international agreements concluded by EU can be contrary to the secondary EU legislation. Thus, while assessing PNR Agreements, the only provisions by reference to which the compatibility of the international agreements may be examined are the provisions of EU primary law, that is to say, the Treaties and the rights set out in the Charter, to the exclusion of secondary law.

2.2.The origins of EU data protection law applicable to assess PNR Agreements

Privacy and data protection – to be more precise: the right to respect for private life and the right to the protection of someone's personal data - are both rather recent expressions of a “[...] universal idea with quite strong ethical dimensions: the dignity, autonomy and unique value of every human

¹⁴² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89–131.

¹⁴³ Consolidated version of the Treaty on the Functioning of the EU, OJ C 326, 26.10.2012, p. 47–390. [hereinafter TFEU]

¹⁴⁴ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 167.

being”¹⁴⁵. Privacy and data protection clarify two features that frequently appear in this context: the need to preclude undue *interference* in private matters, and the need to ensure *adequate control* for individuals over matters that may affect them.¹⁴⁶ The concept of “right to privacy” is ascertained in the Article 8 of the European Convention on Human Rights (hereinafter Convention/ECHR).¹⁴⁷ As “privacy” (Article 7) and “data protection” (Article 8) are mentioned separately in the Charter¹⁴⁸, this also leads to issues regarding the distinction between the two.

The protection of natural persons in relation to the processing of personal data is enshrined in Article 8(1) of the Charter and Article 16(1) of TFEU¹⁴⁹. Article 8 of the Charter not only distinguishes data protection from privacy, but also lays down some specific guarantees in paragraphs 2 and 3.¹⁵⁰ Namely that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on some other legitimate basis laid down by law¹⁵¹; Furthermore, that everyone has the right of access to data which have been collected concerning him or her, and the right to have it rectified; and that compliance with these rules shall be subject to control by an independent authority.¹⁵²

The concept of “personal data” is defined as “[...] any information relating to an identified or identifiable individual (“data subject”)”.¹⁵³ This means that “data protection” is broader than “privacy protection” because it also concerns other fundamental rights and freedoms, and all kinds of data regardless of their relationship with privacy, and at the same time more limited because it merely concerns the processing of personal information, with other aspects of privacy protection

¹⁴⁵ Hustinx, P., “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, supra note 140, p. 2. (Peter Hustinx was European Data Protection Supervisor (2004-2014). This article is based on a course given at the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013. It also draws on material used in multiple articles and speeches published by the author during recent years)

¹⁴⁶ Ibid, p. 2.

¹⁴⁷ European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5, pp. 8(1) everyone has the right to respect for his private and family life, his home and his correspondence. [hereinafter Convention]

¹⁴⁸ Charter of Fundamental Rights of the EU, 7 December 2000, OJ C 364. Article 7 provides the right to respect for his or her private and family life see also 8(1) Everyone has the right to the protection of personal data concerning him or her. [hereinafter Charter]

¹⁴⁹ TFEU, supra note 143, pp. 16(1).

¹⁵⁰ Charter, op. cit., pp. 8.

¹⁵¹ Ibid., pp. 8(2).

¹⁵² Ibid, pp. 8(3).

¹⁵³ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108, pp. 2 sub a.

being disregarded.¹⁵⁴ The concept of “private life” in Article 8 of the Convention is still not entirely clear, but its scope has increased considerably.¹⁵⁵ According to the case law of the ECtHR, it is not limited to “intimate” situations, but also covers certain aspects of professional life and behaviour in public, either or not in the past. On the other hand, those cases still often concern specific situations, which involve sensitive information (medical or social services), justified expectations of privacy (confidential use of telephone or email at work) or inquiries by police or secret services.¹⁵⁶ There is no corresponding provision on data protection in the Convention, nevertheless the ECtHR has applied Article 8 of the Convention (covering the right to privacy) to give rise to a right of data protection as well.¹⁵⁷ However, the ECtHR has so far never ruled that any processing of personal data - regardless of its nature or context - falls within the scope of Article 8.¹⁵⁸

In the light of the explanatory notes¹⁵⁹, the rights guaranteed in Article 7 of the Charter correspond to those guaranteed by Article 8 ECHR.¹⁶⁰ Both are examples of classical fundamental rights, where interference is subject to strict conditions.¹⁶¹ The only difference between them is that Article 52 of the Charter contains a more general exception clause.¹⁶²

¹⁵⁴ Hustinx, P, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", supra note 140 p. 7.

¹⁵⁵ See e.g. *Klass v Germany*, ECHR (1978), pp. 28; *Malone v United Kingdom*, ECHR (1984), pp. 82; *Leander v Sweden*, ECHR (1987), pp. 116; *Gaskin v United Kingdom*, ECHR (1989), A-160; *Niemietz v Germany*, ECHR (1992), pp. 251; *Halford v United Kingdom*, ECHR 1997-IV; *Amann v Switzerland*, ECHR 2000-II, and *Rotaru v Romania*, ECHR 2000-V.

¹⁵⁶ Hustinx, P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", op. cit., 140, p. 7.

¹⁵⁷ ECtHR, *Amann v Switzerland*, no. 27798/95, ECHR 2000-II, para. 65, *Rotaru v Romania* [GC] App no 28341/95, ECHR 2000-V, para. 43.

¹⁵⁸ Peter Hustinx, op. cit., p. 7 – also see ECtHR Case: *Khelili v Switzerland*, 18.10.2011, Application 16188/07, pp. 56: 'The storage of data concerning the applicant's private life, including her profession, and the retention thereof, amounted to an interference within the meaning of Article 8, because it was personal data relating to an identified or identifiable individual' (emphasis added). However, the case was about the conservation of data, including a reference to the applicant as a prostitute, for a long period by the police, without a sufficient factual basis. Moreover, in the same judgment, the Court also said that whether the conservation of personal data raises any aspect of private life depends on the particular context in which these data have been collected and retained, the nature of the relevant data, the way in which they are used and processed, and the consequences this may have (pp. 55),

¹⁵⁹ Explanations relating to the Charter of Fundamental Rights of the European Union, document CONVENT 49 of 11.10.2000, explanation on Article 7. The Bureau of the Convention prepared these explanations for each article of the Charter. They were intended to clarify the provisions of the Charter, indicating the sources and scope of each of the rights set out therein. They had initially no legal value and were only published for information.

¹⁶⁰ Hustinx, P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", supra note 140, p. 16.

¹⁶¹ Ibid., p. 16

¹⁶² Ibid., p. 16

The collection of personal data and retention undoubtedly constitutes an interference with the fundamental rights to the protection of private life and to the protection of personal data.¹⁶³ It is clearly emphasized by the case law of the European Court of Human Rights (hereinafter ECtHR). For instance, in the cases *Rotaru v. Romania*¹⁶⁴, *Amann v. Switzerland*¹⁶⁵ and *Marper v. UK*¹⁶⁶: the ECtHR indicated that the storing of information relating to an individual's private life and the use of it amount to interference with the right to respect for private life secured in Article 8 of the ECHR. Every transmission of personal data from one authority to another, including the subsequent use of such data, constitutes yet another separate interference with individual rights under Article 8 of the ECHR.¹⁶⁷ In a case, *Marper v. UK*, ECtHR stated that all three categories of the personal information retained by the authorities, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter Data Protection Convention or Convention 108)¹⁶⁸ as they relate to identified or identifiable individuals.¹⁶⁹ The Court considered that, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constituted an interference with the right to respect for private life.¹⁷⁰ ECtHR in a case *Amann v. Switzerland* noted that creation and storing of information card¹⁷¹

¹⁶³ Case: *Amann v. Switzerland*, supra note 155, pp. 69-70, see also Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (Vienna, 14 June 2011), p. 6.

¹⁶⁴ Case: *Rotaru v. Romania* (28341/954), 29 June 2006, pp. 46.

¹⁶⁵ Case: *Amann v. Switzerland*, op. cit., pp. 69-70

¹⁶⁶ Case: *S. and Marper v. The United Kingdom* (30562/04 and 30566/04), 4 December 2008, pp. 67

¹⁶⁷ Case: *Amann v. Switzerland*, op. cit., pp. 179

¹⁶⁸ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108, pp. 1. The purpose of the Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection'). Convention has now been ratified by 46 countries, including all EU Member States, most Member States of the Council of Europe and one non-Member State (Uruguay).

¹⁶⁹ Case: *S. and Marper v. The United Kingdom*, supra note 166, pp. 68

¹⁷⁰ *Ibid.*, pp. 86

¹⁷¹ Case: *Amann v. Switzerland* (27798/95) [2000], supra note 155, pp. 7-12. The applicant, who was born in 1940, was a businessman living in Switzerland. In the early 1980s he imported depilatory appliances into Switzerland which he advertised in magazines. On 12 October 1981 a woman telephoned the applicant from the former Soviet embassy in Berne to order a "Perma Tweez" depilatory appliance. That telephone call was intercepted by the Federal Public Prosecutor's Office (*Bundesanwaltschaft* – "the Public Prosecutor's Office"), which then requested the Intelligence Service of the police of the Canton of Zürich to carry out an investigation into the applicant and the goods he sold. The report drawn up by the police of the Canton of Zürich in December 1981 stated that the applicant, who had been registered in the Commercial Registry since 1973, was in the aerosols business. It stated that "Perma Tweez" was a

containing data relating to the applicant's private life was filled in by the Public Prosecutor's Office and stored in the Confederation's card index. Therefore, the ECtHR concluded that both the creation of the impugned card by the Public Prosecutor's Office and the storing of it in the Confederation's card index amounted to interference with the applicant's private life which cannot be considered to be "in accordance with the law" since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration.¹⁷² It follows that there has been a violation of Article 8 of the Convention.

Thus, ECHR¹⁷³ provides that interference can be justified if certain conditions are met: that is to say, if:

- 1) Interference is "in accordance with the law". A key requirement for a sufficient legal basis is that the interference is foreseeable. Rules of a very general nature do not meet this standard.¹⁷⁴ On the contrary, a legal basis for the collection, storage, and disclosure of personal information must lay down the limits of these powers, and in particular the necessary safeguards against abuse and disproportionate measures¹⁷⁵. In the *M.M.* case¹⁷⁶ the ECtHR summed this up as follows: "The greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data".

battery-operated depilatory appliance; a leaflet describing the appliance was appended to the report. On 24 December 1981 the Public Prosecutor's Office drew up a card on the applicant for its national security card index on the basis of the particulars provided by the police of the Canton of Zürich. In 1990 the public learned of the existence of the card index being kept by the Public Prosecutor's Office and many people, including the applicant, asked to consult their card.

¹⁷²Ibid., pp. 78 -80: Swiss law, both before and after 1990, expressly provided that data which turned out not to be "necessary" or "had no further purpose" should be destroyed (section 66(1 *ter*) FCPA, section 414 of the Federal Council's Directives of 16 March 1981 applicable to the Processing of Personal Data in the Federal Administration and Article 7 of the Federal Decree of 9 October 1992 on the Consultation of Documents of the Federal Public Prosecutor's Office).

In the instant case the authorities did not destroy the stored information when it emerged that no offence was being prepared, as the Federal Court found in its judgment of 14 September 1994.

¹⁷³ Convention, *supra* note 147, pp. 8(2).

¹⁷⁴ Case *Amann v Switzerland*, *supra* note 155, pp. 76.

¹⁷⁵ Case *Rotaru v Romania*, *supra* note 155, pp.57 ff.; *Segerstedt-Wiberg and Others v Sweden* App no 62332/00, ECHR 2006-VII, paras 76 ff.; *M.M. v UK* App no. 24029/07 (13 November 2012), paras 195 ff.

¹⁷⁶ ECtHR, *M.M. v UK* App no. 24029/07 (13 November 2012), para. 200.

- 2) Interference pursues one or more of the legitimate aims referred to in paragraph 8(2)¹⁷⁷ which are laid down exhaustively in the Convention. The EU Charter is phrased more openly, and allows for objectives of general interest recognized by the Union and for the need to protect the rights and freedoms of others.¹⁷⁸ Therefore, the Court of Justice has recognized the transparency of the use of public funds as a legitimate objective for the publication of agricultural subsidies to individual farmers, since it found that such publication contributes to the appropriate use of public funds, and enables citizens to participate more closely in the public debate about agricultural policy¹⁷⁹ even though transparency as such is not mentioned as one of the legitimate aims that can justify interference with the right to privacy under the Convention on Human Rights; and is
- 3) Interference is “necessary in a democratic society” to achieve those aims.¹⁸⁰ The most difficult test of any justification is whether the interference is necessary in a democratic society. Any interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued. In this connection, ECtHR considers that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved.¹⁸¹ For instance, it was disproportionate to keep information related to political activities that happened more than 30 years earlier in a secret police register¹⁸². The same applies to information about being a member of a radical political party if this party has not employed illegal means in over 30 years of political activity¹⁸³. The EU Court of Justice recently took a more procedural approach. It did not exclude that the publication of agricultural subsidies to individual farmers might be proportionate, but stressed repeatedly that the legislator had not demonstrated that it sought to strike a fair balance between the interests of the farmers and the aim of transparency.¹⁸⁴

¹⁷⁷Limitation is in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

¹⁷⁸ Charter, *supra* note 148, pp. 52(1)

¹⁷⁹ CJEU, Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 67–71.

¹⁸⁰ Convention, *supra* note 147, pp. 8(2).

¹⁸¹ Case *Segerstedt-Wiberg and Others v Sweden*, *supra* note 175, pp. 88.

¹⁸² *Ibid.*, pp. 90.

¹⁸³ *Ibid.*, 9.

¹⁸⁴ Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert*, *supra* note 179, pp. 79–83.

Nonetheless, the CJEU noted that since the Lisbon Treaty had entered into force, the validity of the obligations had first of all to be assessed in the light of the Charter.¹⁸⁵ Therefore, it is necessary to discuss the conditions for the justification of interference under the Charter.

It follows from the Article 52(1) of the Charter that, to be held to comply with EU law, a limitation on the exercise of right to respect for private life and right to the protection of personal data must, in any event, satisfy three conditions: 1) the limitation must be “provided for by law”¹⁸⁶ in other words the measure in question must have a legal basis; 2) the limitation must “refer to an objective”¹⁸⁷ of public interest, recognised as such by the EU¹⁸⁸; 3) the limitation “may not be excessive: first, it must be necessary and proportional to the aim sought; second, the ‘essential content’, that is, the substance, of the right or freedom at issue must not be impaired”¹⁸⁹. As it was discussed before, the only difference between justification of interference ascertained in the Convention and the Charter is that Article 52 of the Charter contains a more general exception clause.¹⁹⁰

In the light of these two fundamental rights ascertained under the Charter it is worth mentioning Data Retention¹⁹¹ case, which explains some of the provisions of EU primary law.¹⁹² The main objective of the Data Retention Directive¹⁹³ was to harmonize Member States’ provisions concerning the retention of certain data which were generated or processed by providers of publicly

¹⁸⁵ Ibid, pp. 45-46

¹⁸⁶ Case C-407/08 P Knauf Gips v Commission [2010] ECR I-6375, pp. 91.

¹⁸⁷ Included in those objectives are those pursued in the context of the Common Foreign and Security Policy (hereinafter CFSP), and referred to in Article 21(2)(b) and (d) Treaty on the EU (hereinafter TEU), namely to support democracy, the rule of law and human rights, principles of international law as well as sustainable development of developing countries with the essential objective of eradicating poverty;

¹⁸⁸ Consolidated version of the Treaty on EU, OJ C 326, 26.10.2012, p. 13–390, Case T-187/11 Mohamed Trabelsi and Others v Council of the EU [2013], ECLI:EU:T:2013:273, pp. 80.

¹⁸⁹ Case T-187/11 Mohamed Trabelsi and Others v Council of the EU, *ibid.*, pp. 81.

¹⁹⁰ Hustinx, P., “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”, *supra* note 140, p. 16

¹⁹¹ Joined Cases C-293/12 and C-594/12 [2014], ECLI:EU:C:2014:238. These requests for a preliminary ruling concern the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

¹⁹² The High Court (Ireland) and the Verfassungsgerichtshof (Constitutional Court, Austria) were asking the Court of Justice to examine the validity of the Directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data. The Verfassungsgerichtshof has before it several constitutional actions brought by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants. Those actions seek the annulment of the national provision which transposes the directive into Austrian law.

¹⁹³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

available electronic communications services or of public communications networks¹⁹⁴ for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism.¹⁹⁵ The Court observed “[...] that data taken as a whole, may provide very precise information on the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented by them”¹⁹⁶. Furthermore, The Court stated that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the Directive has interfered in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.¹⁹⁷ Furthermore, the fact that data were retained and subsequently used without the subscriber or registered user being informed was likely to generate in the persons concerned a feeling that their private lives were the subject of constant surveillance.¹⁹⁸

The Court then examined whether such an interference with the fundamental rights at issue could have been justified under Article 52(1) of the Charter.¹⁹⁹ It stated that the retention of data required by the Directive was not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data as the only data traffic data were retained.²⁰⁰

As regards the necessity of retention of data, “[...] the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques”.²⁰¹ However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being

¹⁹⁴ Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, PRESS RELEASE No 54/14, Luxembourg, 8 April 2014, p. 1. <
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>> [last accessed 12-27-2016]

¹⁹⁵ Ibid. the Data Retention Directive provided the electronic communications services and public communications networks providers had to retain traffic and location data as well as related data necessary to identify the subscriber or user. However, it did not permit the retention of the content of the communication or of information consulted.

¹⁹⁶ Joined Cases C-293/12 and C-594/12 [2014], op. cit., pp. 27.

¹⁹⁷ Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, supra note 194, p. 1.

¹⁹⁸ Ibid, p. 1, 2.

¹⁹⁹ Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

²⁰⁰ Joined Cases C-293/12 and C-594/12, supra note 191, pp. 39

²⁰¹ Ibid. pp. 51.

considered to be necessary for the purpose of that fight.²⁰² So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.²⁰³ In that regard, it should be considered that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is of great importance for the right to respect the private life nourished in Article 7 of the aforementioned Charter²⁰⁴. Therefore, according to the Court, the retention of data for the purpose of their possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security.²⁰⁵

It was necessary to verify if the proportionality of the existing interference. In that regard, "[...] the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"²⁰⁶ Thus, with regard to judicial review of compliance with those conditions and depending on a number of factors, such as, the area concerned, the nature of the right at issue guaranteed by the Charter, seriousness of the interference and the object pursued by the interference, the extent of the EU legislature's discretion may be limited.²⁰⁷ Therefore, the EU legislation must lay down clear and precise rules which govern the scope and application of the measures and impose minimum safeguards so that the persons concerned have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data²⁰⁸. As a result, the Court stated that, by adopting the Data Retention Directive, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality.²⁰⁹

²⁰² Ibid., pp. 51.

²⁰³ Ibid., pp. 52, see also case C-473/12 IPI EU:C:2013:715, pp. 39.

²⁰⁴ Joined Cases C-293/12 and C-594/12 [2014], op. cit., pp. 53.

²⁰⁵ Joined Cases C-293/12 and C-594/12, supra note 191, pp. 41

²⁰⁶ Ibid., pp. 46, see also case C-343/09 Afton Chemical EU:C:2010:419, paragraph 45; Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 Nelson and Others EU:C:2012:657, paragraph 71; Case C-283/11 Sky Österreich EU:C:2013:28, paragraph 50; and Case C-101/12 Schaible EU:C:2013:661, paragraph 29).

²⁰⁷ Joined Cases C-293/12 and C-594/12, op. cit. pp. 47

²⁰⁸ Ibid., pp. 54

²⁰⁹ Court of Justice of the EU, "The Court of Justice declares the Data Retention Directive to be invalid", supra note 194, p. 2.

The Court noted that the biggest and the most serious interference of the Directive with the fundamental rights at issue was not limited to what was strictly necessary for the following reasons: 1) the Directive covered, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime²¹⁰; 2) the Directive did not lay down any objective criterion ensuring that the competent national authorities would have access to the data and that they would be able use it only for the purposes of prevention, detection or criminal prosecutions concerning offences.²¹¹ On the contrary, the Directive simply referred in a general manner to ‘serious crime’ as defined by each Member State in its national law.²¹²

3) As regards the data retention period, the Directive imposed a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued or according to the persons concerned.²¹³ The Directive did not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.²¹⁴ Therefore, it follows from the above that Directive did not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.²¹⁵

The Court additionally stated that, the Directive did not confer sufficient safeguards to ensure effective protection against the risk of abuse and against any unlawful access and use of the data²¹⁶. It did not ensure the irreversible destruction of the data at the end of their retention period²¹⁷. Not to mention, the Directive did not require that the data would be retained within the EU.²¹⁸ Furthermore, the Directive did not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such control, carried out on the basis of EU law, is an essential component of the protection of

²¹⁰ Joined Cases C-293/12 and C-594/12, *op. cit.*, pp. 57, 58, 59.

²¹¹ *Ibid.*, pp. 60.

²¹² Joined Cases C-293/12 and C-594/12, *supra* note 191, pp. 60.

²¹³ *Ibid.*, pp. 63.

²¹⁴ Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, *supra* note 194, p. 2.

²¹⁵ Joined Cases C-293/12 and C-594/12 [2014], *op. cit.*, pp. 65.

²¹⁶ Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, *op. cit.*, p. 2.

²¹⁷ *Ibid.*, p. 2.

²¹⁸ Joined Cases C-293/12 and C-594/12, *op. cit.*, pp. 65.

individuals²¹⁹. Having regarded to all the foregoing considerations, it was finally held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.²²⁰

To summarize, the ‘right to privacy’ is ascertained in the Article 8 of the Convention. As “right to privacy” is mentioned in the Article 7 of the Charter and “right to data protection” is mentioned in the separate Article 8 of the Charter and Article 16(1) of TFEU. There is no corresponding provision on data protection in the Convention. Nevertheless the ECtHR has applied Article 8 of the Convention to give rise to a right of data protection as well. Nonetheless, the rights guaranteed in Article 7 of the Charter correspond to those guaranteed by Article 8 ECHR. Both are classical fundamental rights, where interference is subject to strict conditions. Nonetheless, since the Lisbon Treaty had entered into force, the validity of the obligations has first of all to be assessed in the light of the Charter. It follows from the Article 52(1) of the Charter that, to be held to comply with EU law, a limitation on the exercise of right to respect for private life and right to the protection of personal data must, in any event, satisfy three cumulative conditions. Limitations must be “provided for by law” in other words the measure in question must have a legal basis. Limitations must refer to an EU recognised objective of public interest. And limitation may not be excessive: it must be necessary and proportional to the aim sought; and the substance, of the right or freedom at issue must not be undermined. In any case, the limitations must be both clearly defined, and necessary and proportionate. Thus, in order to comply with Articles 7, 8 of the Charter interference detected by the PNR Agreements to the “right to privacy” and “right to data protection” has to meet essential fundamental requirements of necessity and proportionality.

2.3.Joint Reviews of the PNR Agreements

As it was mentioned before, in a hierarchy of norms in EU law, international agreements concluded by the EU are subordinate to primary legislation therefore they cannot contravene EU primary law. Under Article 218(11) TFEU, the only provisions by reference to which the compatibility of the agreements may be examined are the provisions of EU primary law, that is to say, in this instance,

²¹⁹ Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, *op. cit.*, p. 3.

²²⁰ Joined Cases C-293/12 and C-594/12, *op. cit.* pp. 69.

the Treaties and the rights set out in the Charter to the exclusion of secondary law.²²¹ It was established in the previous section that PNR Agreements has to be assessed in the light of the Article 7, 8 and 52(1) of the Charter. If PNR international agreements were found to be incompatible with established primary law they would be declared invalid. As the first step PNR Agreements themselves provide joint reviews for the purpose of revising implementation of the Agreements, both Parties policies and practices towards PNR data for the purpose of contributing effective operation and privacy protection of processing PNR.²²² Consequently, if unjustified interference with the right to privacy and personal data protection is detected, in order to be compatible with primary law, the PNR agreements would have to be brought up to date and/or some of their present terms would have to be deleted so that it did not exceed what was strictly necessary in order to achieve their objectives.

Under new 2012 EU-USA, 2014 EU-Canada and 2012 EU-Australia PNR Agreements joint review of the implementation of the Agreements must take place one year after their entry into force and regularly thereafter as jointly agreed.²²³ Further, the Parties jointly evaluate the Agreement four years after its entry into force.²²⁴ The Parties advise each other regarding the enactment of any legislation that materially affects the implementation of this Agreement.²²⁵ Furthermore, Parties jointly determine in advance the modalities and terms of the joint review and shall communicate to each other the composition of their respective teams.²²⁶ These teams may include appropriate experts on data protection and law enforcement.²²⁷

For the purpose of the joint review, the EU is represented by the European Commission and accordingly by competent authority from contracting parties.²²⁸ Subject to applicable laws, participants in the joint review are required to have appropriate security clearances and to respect the

²²¹ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 167.

²²² 2007 EU-USA PNR Agreement, *supra* note 69, Title X, US letter to EU.

²²³ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 23(1), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(2), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(2).

²²⁴ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 23(1), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(3), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(4).

²²⁵ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 22, 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(1), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(1).

²²⁶ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 23(2), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(4), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(3).

²²⁷ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 23(2), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(4), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(3).

²²⁸ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 23(2), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(4), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(3).

confidentiality of the discussions, furthermore, for the purpose of joint review competent authorities from contracting parties ensure appropriate access to relevant documentation, systems, and personnel.²²⁹ Following the joint review, the European Commission presents a report to the European Parliament and the Council of the EU as well as other respective parties are given an opportunity to provide written comments which are attached to the report.²³⁰

Regarding past joint reviews, 2004 EU-USA PNR Agreement was reviewed in 2005²³¹. The outcome of the joint review showed that, as of the date of the Joint Review²³² the Department of Homeland Security Bureau of Customs and Border Protection (hereinafter CBP) was in substantial compliance with the conditions set out in the Undertakings²³³ attached to 2004 EU-USA PNR Agreement.²³⁴ The EU team also found that it took some time before compliance was achieved, and that CBP had received substantial assistance to achieve compliance from the Department of Homeland Security Privacy Office (hereinafter DHS Privacy Office)²³⁵. Some areas of concern were identified as well as some positive findings where CBP significantly went beyond what was necessary in order to comply with the Undertakings.²³⁶ Particularly in the Joint Review CBP undertook to permanently delete any sensitive data collected between March 2003 and May 2004, although the Joint Review was not concerned with this period²³⁷. The EU Joint Review team recommended “[...] CBP to provide its officers with clearer guidance as to the meaning and interpretation of the notion of “serious crimes that are transnational in nature”, to contribute more actively to the implementation of a ‘push’²³⁸ system and to improve information to passengers on the transfer of PNR data”²³⁹. The DHS Privacy Office report indicated that upon conclusion of the

²²⁹ 2012 EU-USA PNR Agreement, *supra* note 11 , pp. 23(2), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(4), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(3).

²³⁰ 2012 EU-USA PNR Agreement, *supra* note 11 , pp. 23(3), 2014 EU-Canada PNR Agreement, *supra* note 12, pp.26(5), 2012 EU-Australia PNR Agreement, *supra* note 11, p. 24(5).

²³¹ 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 14 May 2004, Brussels, 12.12.2005, COM (2005) final.

²³² 20 and 21 September 2005.

²³³ On 11 May 2004, the Department of Homeland Security Bureau of Customs and Border Protection (CBP) issued Undertakings which clarified and defined the conditions for the transfer of PNR passengers' data to US authorities, ensuring that such transfer would have taken place in compliance with Community principles concerning individuals' right to privacy.

²³⁴ Commission Staff Working Paper, *op. cit.* 12.12.2005, COM (2005) final, pp. 4.

²³⁵ *Ibid.*, pp. 4.

²³⁶ *Ibid.*, pp. 4.

²³⁷ *Ibid.*, pp. 4.

²³⁸ “push” system –requires that the PNR data are selected and transferred by airline companies to US authorities

²³⁹ Commission Staff Working Paper, *op. cit.* pp. 4.

Joint Review CBP would update field guidance in order to include recommendations that may be made by the Joint Review team.²⁴⁰

Furthermore, the 2007 EU-USA PNR Agreement was jointly reviewed in 2010²⁴¹. There were four parameters to the review: the implementation of the agreement and the letter conducted by the U.S., U.S. and EU PNR policies and practices, instances in which sensitive data has been accessed and the discussions of the representatives of Member States sustaining PNR systems.²⁴² Another parameter of the review was to verify that the Agreement actually serves its purpose and indeed contributes to the fight against terrorism and serious crime.²⁴³

The outcome of this joint review was that “PNR actually serves the purpose of supporting the fight against terrorism and serious crime”²⁴⁴. The EU team also found that DHS generally implemented the Agreement.²⁴⁵ It was also found that the majority of undertaken commitments were implemented accordingly to the Agreement. Furthermore, DHS respected its obligations as regards the rights of passengers²⁴⁶. It was especially important to note that “[...] the U.S. had transposed its commitments towards the EU into domestic rules through the publication of a System of Records Notice in the Federal Register”²⁴⁷. However, the implementation of some commitments was challenging. DHS was again encouraged to intensify its efforts to ensure that all carriers use the push method²⁴⁸. The most worrying areas related to the use of PNR data for the purposes of customs and immigration, large numbers and method of pursuing the ad hoc requests²⁴⁹ and the non-proactive²⁵⁰ realization of the mutuality and co-operation commitment by sharing analytical

²⁴⁰ Ibid., pp. 4.

²⁴¹ Report on the joint review of the implementation of the Agreement between the EU 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, Brussels, 7.4.2010.

²⁴² Ibid., pp. 1.

²⁴³ Ibid., pp. 1.

²⁴⁴ Ibid., pp. 4.

²⁴⁵ Ibid., pp. 4.

²⁴⁶ Ibid., pp. 4.

²⁴⁷ Ibid., pp. 4.

²⁴⁸ Ibid, 7.4.2010, pp. 4.

²⁴⁹ In cases where DHS has a hit (an alert) on the basis of data found in the first transmission at 72 hours, or if it has intelligence that a certain individual is due to fly on a specific flight, DHS requires that the data is transmitted at additional intervals to the four standard transmissions, in order to have frequent updates of the situation. These updates are called ‘ad hoc requests’.

²⁵⁰ pro-active: using data for analysing and creating assessment criteria, which can be used later for a pre-arrival and pre-departure assessment of passengers

information flowing from PNR data with Members States, Europol and Eurojust²⁵¹. Therefore, it was agreed that a follow up review would be carried out in the course of 2011 to further monitor these matters.²⁵²

In 2012 EU-USA entered into a new 2012 EU-USA PNR Agreement according to which the Parties shall jointly review the implementation of the Agreement one year after its entry into force and regularly thereafter as jointly agreed.²⁵³ In line with this requirement, the first joint review of the Agreement was carried out one year after its entry into force on 1 July 2012, i.e. in Washington on 8 and 9 July 2013.²⁵⁴

As an outcome of the joint review, The EU team found that DHS implemented the Agreement in accordance with the terms of the Agreement.²⁵⁵ In particular, the DHS respected its obligations as regards the access rights of passengers and as a regular oversight mechanism in place to guard against unlawful non-discrimination.²⁵⁶ It was especially important to note that the U.S. had transposed its commitments towards the EU into domestic rules through the publication of a System of Records Notice in the U.S. Federal Register.²⁵⁷ Notwithstanding that, the implementation of some commitments was technically and operationally challenging. In particular, as regards the implementation of the push method. DHS was again convened to intensify its efforts to ensure that all carriers use the push method by 1 July 2014²⁵⁸. Besides DHS was again called to further improve implementation of the reciprocity commitment on sharing individual PNRs and analytical information flowing from PNR data with Members States, Europol and Eurojust.²⁵⁹ It was also

²⁵¹ Report on the joint review, supra note 241, pp. 4.

²⁵² Ibid., pp. 4.

²⁵³ 2012 EU-USA PNR Agreement, supra note 11, pp. 23(1).

²⁵⁴ Joint Review of the implementation of the Agreement between the EU and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security Accompanying the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the EU and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, {COM(2013) 844 final}, Brussels, 27.11.2013, SEC(2013) 630 final.

²⁵⁵ Ibid., pp. 3

²⁵⁶ Ibid., pp. 3

²⁵⁷ Ibid., pp. 3

²⁵⁸ Ibid., pp. 3

²⁵⁹ Ibid., pp. 3

proposed to organize the next joint review of the Agreement during the first half of 2015²⁶⁰. However, as of 31 December 2016 there is no new joint review released.

The 2012 EU-Australia PNR Agreement fully entered into force on 1 June 2012.²⁶¹ Under new Agreement Parties were supposed to jointly review the implementation of the Agreement and any matters related thereto one year after its entry into force and regularly thereafter.²⁶² In line with this requirement, the first joint review of the Agreement was carried out in Canberra on 29/30 August 2013²⁶³. As the outcome of the joint review, the overall finding was that Australia had fully implemented the Agreement in line with the conditions set out therein.²⁶⁴ In fact, according to the findings it was concluded that Australia respected its obligations as regards the data protection safeguards under the Agreement, and processed PNR data in compliance with the strict conditions set out in the Agreement²⁶⁵. As a matter of fact, the sensitive PNR data which was obtained under the Agreement was not processed by Australia. The identification and deletion processes of sensitive data have been actively pursued to be further improved²⁶⁶. The targeted way in which Australia assessed PNR data against risk indicators usefully minimized the access to personal data.²⁶⁷ Furthermore, the processing of PNR data under the Agreement was subject to a high level of independent oversight by the Office of the Australian Information Commissioner.²⁶⁸

However, it was noted that law enforcement cooperation based on the sharing of analytical information obtained from PNR data required more attention.²⁶⁹ Australia same as US was invited to increase its mutual cooperation by sharing analytical information obtained from PNR data with Member States and, where appropriate, with Europol and Eurojust pro-actively²⁷⁰. At the same time, recipients of such information on the EU side should have provided adequate feedback to the

²⁶⁰ Joint Review of the implementation of the Agreement, supra note 255, pp. 3

²⁶¹ 2012 EU-Australia PNR Agreement, supra note 11.

²⁶² Ibid, pp. 24(2).

²⁶³ Joint Review Report of the implementation of the Agreement between the EU and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service Accompanying the Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the EU and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service {COM(2014) 458 final}, Brussels, 10.7.2014, SWD(2014) 236 final.

²⁶⁴ Ibid., pp. 3.

²⁶⁵ Ibid., pp. 3.

²⁶⁶ Ibid., pp. 3.

²⁶⁷ Ibid., pp. 3.

²⁶⁸ Ibid., pp. 3.

²⁶⁹ Ibid., pp. 3.

²⁷⁰ Joint Review Report of the implementation of the Agreement between the EU and Australia, supra note 263, pp. 3.

Australian Customs and Border Protection Service (hereinafter ACBPS) on the use of this information and the results achieved.²⁷¹ Australia was also requested to set up a reporting mechanism that would enable Australia to inform Member States if PNR data received under the Agreement, or analytical information containing such data, was eventually shared with a third country²⁷². Australia should have continued to ensure that the safeguards set out in the Agreement were also afforded to PNR data, which was shared with other areas of Australian government authorities.²⁷³ It was envisaged to combine the next joint review of the Agreement with the joint evaluation of the Agreement in mid-2016.²⁷⁴ However, as of 31 December 2016 is no new joint review released.

Joint review of 2006 EU-Canada Agreement took place in 2008, unfortunately, it cannot be publicly accessed.²⁷⁵ As it was mentioned before, the EU and Canada signed the new agreement on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Canadian competent authorities on 25 June 2014²⁷⁶. Following signing of the Agreement Council of the EU requested European Parliament to approve it.²⁷⁷ However, in November 2014 EU Parliament requested the Court to deliver an opinion on the agreement. The Opinion should enable the Parliament to decide on the Council's request of July 2014 to approve the proposal for a decision on the conclusion of the new agreement envisaged.²⁷⁸

To sum up, every EU PNR Agreement concluded with US, Australia and Canada has almost identical provisions regulating the joint reviews of Agreements. In fact, provisions on Joint reviews are envisaged for the purpose of revising implementation of the Agreements, both Parties policies and practices towards PNR data for the purpose of contributing effective operation and privacy protection of processing PNR. That is to say, to verify the fulfilment of obligations undertaken by US, Australia and Canada competent authorities in order to comply with Agreements. Consequently, non-compliance with undertaken obligations may result in the suspension or termination of

²⁷¹Ibid., pp. 3.

²⁷²Ibid., pp. 3.

²⁷³Ibid., pp. 3.

²⁷⁴Ibid., pp. 3.

²⁷⁵F. de Londras, Doody, J. "The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism", Routledge, Taylor&Francis Group, 2015. , p. 223

²⁷⁶ Council of the EU, Signature of the EU-Canada agreement on Passenger Name Records (PNR), supra note 82.

²⁷⁷ Ibid.

²⁷⁸ Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU, Opinion 1/15, 2015/C 138/32.

Agreements or non-compliance with EU primary law. As regards joint review of EU-Canada PNR Agreement it cannot be publicly accessed. Even though the overall outcomes in all the Joint reviews resulted in conclusions that USA and Australia had implemented the Agreements in line with the conditions set out therein it was acknowledged that the implementation of some commitments was technically and operationally challenging. Competent authorities were called to pay more attention to certain provisions. In particular, it has to be observed that, all the joint reviews undertaken by Parties as regards EU-USA PNR Agreements were concerning almost identical provisions to be improved. This questions the real added value of the effectiveness of this procedure. In particular, DHS has invited to contribute more actively to the implementation of a “push” system in all the joint reviews which indicates that DHS did not intensify its efforts to fulfil undertaken obligations to ensure that all carriers use the push method. Both 2005 and 2010 Joint reviews concerned the imprecise and unclear purpose limitation of the 2004 and 2007 EU-PNR Agreements, that is to say, the most worrying areas related to the use of PNR data for the purposes of customs and immigration. Therefore clearer guidance as to the meaning and interpretation of the notion of “serious crimes that are transnational in nature” were asked to be provided. Both 2010 and 2012 Joint reviews called to further improve implementation of the reciprocity commitment on sharing individual PNRs and analytical information flowing from PNR data with Member States, Europol and Eurojust. Australia same as US was invited to increase its mutual cooperation by sharing analytical information obtained from PNR data with Member States and, where appropriate, with Europol and Eurojust pro-actively. Australia was also requested to set up a reporting mechanism that would enable Australia to inform Member States if PNR data received under the Agreement, or analytical information containing such data, was eventually shared with a third country. Therefore, this raises the question whether PNR Agreements are compatible with EU primary law, to be exact, Article 7, 8 and 52(1) of the Charter.

III. THE COMPATIBILITY OF THE EU-CANADA, EU-USA AND EU AUSTRALIA PNR AGREEMENTS WITH THE EU PRIVACY AND DATA PROTECTION RULES

In the light of Articles 7, 8 and 52(1) of the Charter the first subsection of Chapter 3 provides assessment of necessity of the Agreements concluded by EU with USA, Canada and Australia which is verified in conjunction with the purpose of the Agreements provided therein. Further subsections provide assessment of the proportionality of the mostly criticized provisions of the 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements. In particular, proportionality of provisions such as rather long period of data retention, wide spectrum of the use of data, a large amount of data elements to be collected, disclosure of data to other government authorities and third countries and guarantees for and rights of data subjects. In the light of the recently published Opinion of the Advocate General of the CJEU on compatibility of the 2014 EU-Canada PNR Agreement regarding rights guaranteed under EU treaties, in particular the rights to privacy and data protection, this Chapter first of all focuses on the assessment of the EU-Canada PNR Agreements, following EU-USA PNR Agreements and EU-Australia PNR Agreements.

3.1 Necessity of the PNR agreements concluded by EU with Canada, USA and Australia

In order to ascertain whether the interference with the right to privacy and the right to the protection of private data entailed by the 2012 EU-USA, 2012 EU-Australia and 2014 EU-Canada PNR Agreements at hand are in compliance with the principle of necessity enshrined in the Article 52(1) of the Charter, it is paramount to take a closer look at the purpose of the Agreements provided therein in the first place.

As for the purpose of the Agreement, 2014 EU-Canada PNR Agreement provides a slightly different approach than 2006 PNR Agreement, which was directly referring to a protection of fundamental rights and freedoms. The purpose of the 2014 EU-Canada Agreement is “to ensure the security and safety of the public and prescribe the means by which the data is protected”.²⁷⁹ For the first time in a US-EU PNR Agreements’ history 2012 PNR Agreement provides clearly stated purpose, that is to say, “to ensure security and to protect the life and safety of the public”²⁸⁰. As for the purpose of the 2012 EU-Australia Agreement, it is designed to “ensure the security and safety of the public” while EU-sourced PNR data is transferred to and used by Australian competent authority which is known as Australian Customs and Border Protection Service in the manner in which such

²⁷⁹ 2014 EU-Canada PNR Agreement, supra note 12, pp.1.

²⁸⁰ 2012 EU-USA PNR Agreement, supra note 11, pp. 1

data is protected.²⁸¹ It can be seen that 2012 EU-Australia PNR Agreement along with other PNR Agreements concluded in 2012-2014 concentrate more on ensuring security and safety of the public whilst leaving privacy and data protection in the background while seeking to prevent, combat, repress, and eliminate terrorism and terrorist-related offences, as well as other serious transnational crime when processing, using and transferring EU-sourced PNR data.

Article 52(1) of the Charter provides that limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.²⁸² As it was already mentioned, the CJEU itself stated that as regards the necessity of retention of data it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques.²⁸³ Therefore, the CJEU stated that the retention of data for the purpose of their possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security.²⁸⁴

In that regard, it can be presumed that processing, using, storing and transferring of EU-sourced PNR data by competent US, Canadian and Australian authorities seeking to prevent, combat, repress, and eliminate terrorism and terrorist-related offences, as well as other serious transnational crime genuinely satisfied an objective of general interest, to be exact, public security.

3.2. Proportionality of the PNR agreements concluded by EU with Canada, USA and Australia

The principle of proportionality requires that acts of the EU do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.²⁸⁵ As to the strict necessity for the interference consisting in the Agreement, its assessment must entail ascertaining whether the contracting parties have struck a ‘fair balance’ between the objective of combating terrorism and serious transnational crime and the objective of protecting personal data and respecting the private

²⁸¹ 2012 EU-Australia PNR Agreement, *supra* note 11, pp. 1

²⁸² Charter, *supra* note 148, pp. 52(1)

²⁸³ Joined Cases C-293/12 and C-594/12, *supra* note 293, pp. 51.

²⁸⁴ Joined Cases C-293/12 and C-594/12, *ibid.*, pp. 41

²⁸⁵ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 196

life of the persons concerned.²⁸⁶ Such a fair balance must be capable of being reflected in the terms of the Agreement.²⁸⁷

In order to ascertain whether the interference with the right to privacy and the right to the protection of private data entailed by the 2012 EU-USA, 2012 EU-Australia and 2014 EU-Canada PNR Agreements at hand are in compliance with the principle of proportionality, it is paramount to take a closer look at certain provisions of the Agreements. For the purposes of this analysis, the mostly criticized provisions will be discussed in a following order: 1) the use of PNR data; 2) data elements to be collected; 3) data retention periods; 4) disclosure of data; 5) the guarantees for and rights of data subjects.

3.2.1. Proportionality of the use of PNR data ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements

One of the main elements opposing the proportionality of the 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements at hand is the wide spectrum of the use of PNR data. “Prior to the collection of data in security-related data processing, it is crucial to ascertain for which purposes the data should be used afterwards [...]”²⁸⁸. Therefore, boundaries have to be established within which personal data collected for a given purpose may be processed and may be put to further use”²⁸⁹. In that regard, Commission states that the scope of the use of the data by a third country should be spelt out clearly and precisely in the agreement and should be no wider than what is necessary in view of the aims to be achieved.²⁹⁰

2014 EU-Canada PNR Agreement provides that EU sourced PNR data is processed strictly for the purpose of preventing, detecting, investigating or prosecuting “terrorist offences” or “serious transnational crime”.²⁹¹ The wide scope of offences provided in 2006 EU-Canada PNR Agreement

²⁸⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 207

²⁸⁷ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 207

²⁸⁸ Serge Gutwith, Ronald Leenes, Paul De Hert, Yves Poullet editors, “European Data Protection: In Good Health?” Springer Dordrecht Heidelberg London New York, 2012, Franziska Boehm, Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems, p. 148, also see case *Weber and Saravia v. Germany*, *supra* note 184, pp. 116; and *Rotaru v. Romania*, *supra* note 164, pp. 57;

²⁸⁹ Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, Adopted on 2 April 2003, 00569/13/EN WP 203, p. 4.

²⁹⁰ Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, *supra* note 127, p. 10.

²⁹¹ 2014 EU-Canada PNR Agreement, *supra* note 12, pp.3

was reduced leaving “other serious crimes” behind²⁹² which according to the Commission had allowed PNR data to be used not only for law enforcement and security purposes to fight terrorism and serious transnational crime. Therefore, evidently the 2014 EU-Canada Agreement drew attention to guidelines of the Communication of the Commissions listing the use of PNR data.²⁹³

Regarding “terrorist offences” the 2014 PNR Agreement provides a group of conducts which may be assumed as such, for instance: “an act or omission that may cause a serious risk to the physical or economic security of the public; activities representing an offence pursuant International Conventions and Protocols on terrorism; establishing or participating in a terrorist entity having the above purposes”.²⁹⁴ Under 2014 EU-Canada PNR Agreement “serious transnational crimes” mean offences, which involve more than one country and are punishable in Canada by a maximum deprivation of liberty of at least 4 years or a more serious penalty if so provided under Canadian law, if the crimes are transnational in nature.²⁹⁵ The definition clearly does not cover minor offences. Nonetheless, Advocate General Paolo Mengozzi suggests that to consider that the interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter is limited to what is strictly necessary, the offences within the definition “serious transnational crime” should be listed exhaustively, for example, in an annex to the agreement.²⁹⁶

The 2014 EU-Canada Agreement also provides processing of data in exceptional circumstances to protect vital interests of any individual²⁹⁷. In particular, if “a risk of death or serious injury” or a significant public health risk as required by internationally recognised standards may occur.²⁹⁸ However, those standards are nowhere to be seen and defined. In this way, the Canadian competent authority is authorized to process and transfer PNR data for purpose not properly related to the prevention of and combating terrorism. Furthermore, 2014 EU-Canada PNR Agreement confers on Canada the right to process PNR data, on a case-by-case basis, in order to ensure the oversight or accountability of the public administration which provides legal security of the rights of passengers

²⁹² 2006 EU-Canada PNR Agreement, *supra* note 9, pp. 2.

²⁹³ Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, *op. cit.*, p. 10.

²⁹⁴ Rossi Dal Pozzo, F. “EU Legal Framework for Safeguarding Air Passenger Rights”, *supra* note 21, p. 120.

²⁹⁵ 2014 EU-Canada PNR Agreement, *supra* note 12, pp.3(3).

²⁹⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 235.

²⁹⁷ 2014 EU-Canada PNR Agreement, *supra* note 12, pp.3(4)

²⁹⁸ 2014 EU-Canada PNR Agreement, *supra* note 12, pp.3(4)(a)(b)

whose data is transferred to the Canadian authorities²⁹⁹. The processing of PNR data is “also” permitted, on a case-by-case basis, in order to comply with the subpoena or warrant issued, or an order made, by a court³⁰⁰, although it is not stated in the Agreement that the court must be acting in the context of the purposes of the agreement³⁰¹. As Advocate General Paolo Mengozzi precisely observes, this provision appears to allow the processing of PNR data for purposes unrelated with those pursued by the Agreement and/or possibly in connection with conduct or offences not coming within the scope of that Agreement.³⁰² That is to say, this provision allows extending the possibility of data processing therefore is incompatible with Articles 7 and 8 and Article 52(1) of the Charter because it allows the processing of PNR data to be extended beyond what is strictly necessary, independently of the stated purposes of the Agreement.³⁰³

When comparing the 2004 PNR, 2007 PNR and 2012 EU-USA PNR Agreements the purposes for which the PNR data can be used have been extended. The purpose of the original 2004 EU-USA PNR Agreement was limited to the prevention and combat of terrorism and related crimes, other serious crimes (including organized crime) that are of transnational nature, and flight from warrants or custody for both groups of crimes³⁰⁴. The 2007 EU-USA PNR Agreement extended these purposes to the protection of the vital interests of the data subject or other persons as well as to the use in any criminal judicial proceeding, or as otherwise required by law.³⁰⁵ In this way, USA authorized the processing and transfer of PNR data for purposes not properly related to the prevention of and combating terrorism. These already far reaching purposes were replicated and even more broadened in the new 2012 EU-USA PNR Agreement, which includes “preventing, detecting, investigating, and prosecuting : 1) Terrorist offences and related crimes 2) other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature”. Article 4 of 2012 EU-USA PNR Agreement is divided into 4 paragraphs which entail, on the one hand, a list of definitions of terrorist offences and related crimes (paragraph 1 (a)) and other

²⁹⁹ 2014 EU-Canada PNR Agreement, supra note 12, pp. 3(5)(a)

³⁰⁰ 2014 EU-Canada PNR Agreement, supra note 12, pp. 3(5)(b).

³⁰¹ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 236

³⁰² Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 236

³⁰³ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 237

³⁰⁴ Paragraph 3 of the Undertakings of the 2004 agreement, supra note 233.

³⁰⁵ Paragraph I, US letter to EU, annex to the 2007 agreement, supra note 222.

transnational crimes punishable by a sentence of three years or more (paragraph 1 (b)), and on the other hand, further purposes PNR data may be used for (paragraphs 2 to 4).³⁰⁶ .

It has to be observed that, first of all, provisions in the Agreement does not lay down clear and precise definitions in relation to the nature of the offences in respect of which the US authorities would be entitled to process the PNR data. Even though Agreement specifies the terms “terrorist offences and related crimes” and the catalogue of examples is given, as Prof. Dr. Gerrit Hornung and Dr. Franziska Boehm notifies the use of the wording “including conduct that” when specifying these terms, indicate that the given definitions are only examples of several offences which may fall under the terms “terrorist offences and related crimes”.³⁰⁷ As Dr. Michele Nino rightly noticed the vagueness of the indicated purposes can legitimize a widespread use of PNR data.³⁰⁸

Moreover, what is clearly missing is the word serious instead of “other crimes” because it indicates that every crime with the threshold of three years and is transnational in nature can qualify for PNR data being processed. Even so, the threshold to consider a crime “serious” or as it states in the Agreement “other crime” it is set lower per one year in comparison to 2014 EU-Canada PNR Agreement. Even though the definition clearly does not cover minor offences, this still leads to the inclusion of less serious crimes into the scope of application. However, the list of offences which falls under this definition is not given. To ensure the legal certainty of passengers whose data is transferred to the US authorities, the offences coming within this definition should be listed exhaustively.

Secondly, it can be seen from the 2012 EU-USA PNR Agreement itself that PNR data can be thus used for other purposes not actually related to terrorist offences or other crimes transnational in nature. For instance, PNR may be used and processed on a case-by-case basis or “if ordered by a court”³⁰⁹. This actually indicates the use of PNR for any purposes as long as this use is somehow ordered by a court. Likewise, PNR may be used in order to protect “vital interest of any individual” which indicates that USA competent authority is authorised to use and process PNR data as long as

³⁰⁶ Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security”, supra note 306, pp.3.1.

³⁰⁷ Ibid., pp.3.1

³⁰⁸ Nino, M., “The protection of personal data in the fight against terrorism”, supra note 20, p. 76.

³⁰⁹ 2012 EU-USA PNR Agreement, supra note 11, pp. 4 (2).

any individual is in a view of serious threat however who may not even be properly related to the prevention of and combating terrorism.

Furthermore, the identification of “persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination”³¹⁰ appears to include the use of PNR for a wide range of “border control purposes” considerably enlarging the use of PNR data. Additionally, all provisions mentioned above “shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR”³¹¹. The wording used in this paragraph does not clarify which “other violations of law or indications thereof” are actually meant.³¹² This leaves room for further interpretation with regard to the nature of these offences; that is to say, it is not even clear whether only criminal offences are included.³¹³ Prof. Dr. Gerrit Hornung, Dr. Franziska Boehm preserves the wording suggests however that this is not the case and accordingly, the data could be used in proceedings on administrative offences or even breaches of ordinary civil law.³¹⁴ With regard to criminal offences, this paragraph may render paragraph dealing with “other transnational crimes” meaningless³¹⁵, as there is no mentioning of a minimum threshold for these violations (as opposed to paragraph 1 (b) of Article 4: sentence of three years or more.³¹⁶ As a consequence, aforementioned purposes of the 2012 EU-USA PNR Agreement are not specifically linked and strictly limited to the overarching goal of the prevention, detection and investigation and prosecution of terrorist offences and related crime and other serious transnational crime.

As regards the use of PNR data of the 2012 EU-Australia PNR Agreement, it provides that EU-sourced PNR data will only be used for the prevention, detection, investigation and prosecution

³¹⁰ Ibid., pp. 4 (3).

³¹¹ Ibid., pp. 4 (3).

³¹² Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security “, supra note 306, pp.3.1.

³¹³ Ibid., pp.3.1

³¹⁴ Ibid., , pp.3.1

³¹⁵ 2012 EU-USA PNR Agreement, op. cit., pp. 4 (1)(b).

³¹⁶ Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security “, supra note 306, pp.3.1

of terrorist offences or serious transnational crimes.³¹⁷ 2012 EU-Australia PNR Agreement provides a detailed description of the cases that fall within the definition of these types of offences. This shows far more developed approach towards precise and explicit purpose limitation in comparison with its predecessor and other PNR Agreement, i.e. 2012 EU-USA and 2014 EU-Canada PNR Agreements.

Contrary to the provisions of the 2012 EU-USA PNR Agreement, which empowers the United States to collect and use PNR data to prevent, detect, investigate and prosecute offences punishable with no less than 3 years' imprisonment and of a transnational nature, 2012 EU-Australia PNR Agreement provides that serious transnational crimes means "[...] offence punishable in Australia by a custodial sentence or a detention order for a maximum period of at least 4 years or a more serious penalty and as it is defined by the Australian law, if the crime is transnational in nature"³¹⁸. The same provision was replicated in 2014 EU-Canada PNR Agreement.

Even though, 2012 EU-Australia PNR Agreement clearly does not cover minor offences, the suggestion of Advocate General Paolo Mengozzi to provide exhaustive the list of offences within the definition "serious transnational crime" made in case of 2014 EU-Canada PNR agreement³¹⁹ should also be applied to 2012 EU-Australia PNR Agreement. As it was already mentioned in the analysis of the EU-Canada agreements, the exhaustive list ensures that the interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter in this regard is limited to what is strictly necessary.

The 2012 EU-Australia PNR Agreement also provides that in exceptional cases, PNR data may be processed by Australia for the protection of the vital interests of any individual³²⁰. In particular, if a risk of death, serious injury or threat to health may occur.³²¹ In this way, the Australian customs service may be authorized to process and transfer PNR data for purposes not properly related to the prevention of and combating terrorism.³²² This provision was also replicated in 2014 EU-Canada and 2012 EU-USA PNR Agreements. Additionally, the 2012 EU-Australia allows the processing of PNR data on a case-by-case basis for the "purpose of supervision and

³¹⁷ 2012 EU-Australia PNR Agreement, supra note 11, pp. 3(1).

³¹⁸ Ibid, pp. 3(4).

³¹⁹ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 235.

³²⁰ 2012 EU-Australia PNR Agreement, supra note 11, pp. 3(4).

³²¹ Ibid, pp. 3(4).

³²² Nino, M. "The protection of personal data in the fight against terrorism", supra note 20 p. 80

accountability of public administration and the facilitation of redress and sanctions for the misuse of data where such processing is specifically required by Australian law”³²³. Similar provision was replicated in 2014 EU-Canada PNR Agreement, however, the 2012 EU-Australia PNR Agreement provides even more detailed approach which provides legal security of the rights of passengers whose data is transferred to the Australian authorities. This provision appears to be very precise and rational, providing guarantees to the PNR data owners and ensuring supervision of the use and misuse of data by independent authority which is required by the Article 8(3) of the Charter, therefore, the use of PNR data for the purpose of supervision and accountability of public administration is proportional and compatible with the Articles 7, 8 and 52(1) of the Charter because it does not allow the processing of PNR data to be extended beyond what is strictly necessary, independently of the stated purposes of the Agreement.

Summing up the analysis of the use of data of all PNR Agreements, one must conclude that provisions on the processing of PNR data under 2012 EU-Australia Agreement display a better approach than other PNR Agreements towards strict necessity of the use of PNR data for the prevention of terrorism and serious transitional crimes. However, it still authorises the use of PNR data by Australia for the protection of the vital interests of any individual which is not properly related the prevention of and combating terrorism. Therefore is incompatible with Articles 7 and 8 and Article 52(1) of the Charter as it allows the possibilities of processing PNR data to be extended beyond what is strictly necessary. As for the criticism arguments, the deficiencies pertinent to all PNR agreements may be identified. In order to be limited to what is strictly necessary and to ensure the legal certainty of passengers, all PNR Agreements must be accompanied by an exhaustive list of the offences coming within the definition of “serious transnational crime”. In its current form, the provision under 2014 EU-Canada PNR agreement on the processing of PNR data on a case-by-case basis, in order to protect vital interests of any individual, in order to comply with the subpoena or warrant issued, or an order made, by a court is incompatible with Articles 7 and 8 and Article 52(1) of the Charter because it allows the processing of PNR data to be extended beyond what is strictly necessary, independently of the stated purposes of the Agreement. Similarly, the provision under 2012 EU-USA PNR agreement on the processing of PNR data on a case-by-case basis, in order to protect vital interests of any individual, if it is ordered by a court, for the border control purposes or

³²³ 2012 EU-Australia PNR Agreement, op. cit., pp. 3(5).

other violations of law or indications thereof are detected and by later undermining “criminal offences” is incompatible with Articles 7 and 8 and Article 52(1) of the Charter because it allows processing of PNR data to be extended beyond what is strictly necessary.

3.2.2. Proportionality of the data elements to be collected ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements

Proportionality should be ensured not only as regards to purposes and the type of offence to be monitored, but also in respect of transferable personal data.³²⁴ This subsection provides assessment of the obligation under 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements to ensuring that data to be transferred was limited to what was necessary and proportional as regards Article 7,8 and 52(1) of the Charter.

In respect of data elements to be collected, the 29 WP repeatedly admonished to ensure conformity with the principle of proportionality, the minimum amount of EU-sourced PNR data elements should be transferred to the third countries.³²⁵ Therefore, data should be limited to the following information: “PNR record locator code³²⁶, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history³²⁷, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data

³²⁴ Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data* (13 06 2003), p. 7.

³²⁵ Article 29 Data Protection Working Party, *ibid.*, p. 7.

³²⁶ PNR record locator is a Computer Reservation System’s unique identification for the particular Passenger Name Record consisting of six letters or numbers (G. Todd, S. Rice, *A Guide to Becoming a Travel Professional* (Cengage Learning, 2003), p. 57

³²⁷ A no-show is a clause that some airlines include in their terms of use. It basically means that a user not showing up for the outbound flight will be considered a no-show, and all the connecting flights associated with this one, even a return flight, will be cancelled and no refund will apply. (Mark Feldman “The Travel Adviser: No show, no fly”, 09/26/2015, < <http://www.jpost.com/Not-Just-News/The-Travel-Adviser-No-show-no-fly-419193>> [last accessed 12/10/16]

with regard to the aforementioned items”³²⁸. According to the recommendations of the 29 WP, transfer of sensitive data³²⁹ should be excluded.³³⁰

As for the data elements to be transferred, the 2014 EU-Canada PNR Agreement provides a reduced list consisting of 19 data elements³³¹ when comparing to 25 in its predecessor of 2006³³². Without there being any need to examine individually and exhaustively the 19 categories of PNR data set out in the Annex to the Agreement, it is common ground that they deal with the passenger’s identity, nationality and address, contact information (address of residence, email address, telephone number) about the passenger who made the reservation, payment information, including, where appropriate, the number of the credit card used to reserve the flight, information relating to luggage.³³³ Advocate General Paolo Mengozzi accurately notes that the list actually consists of data elements such as “all available contact information”, “all baggage information” and “general remarks” which was excluded under its predecessor.³³⁴ “General remarks”³³⁵ such as OSI, SSI and SSR information, for instance, meal preference and special dietary requirements or request for a wheelchair may actually reveal data related to ethnic origin, religious beliefs or health.³³⁶ That is to say, aforementioned PNR data apt to contain such sensitive data, which should be explicitly excluded³³⁷. Therefore, 2014 EU-Canada PNR Agreement goes beyond what is strictly necessary by including in its scope the transfer of PNR data that is apt to contain sensitive data, which in material terms allows information about the health or ethnic origin or religious beliefs of the passenger concerned and and/or of those travelling with him to be disclosed. Thus, is incompatible with Articles 7, 8 and 52(1) of the Charter.

³²⁸ Article 29 Data Protection Working Party, *supra* note 324, p. 7.

³²⁹ "Sensitive data" means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sex life. Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, L 186, 14/07/2012, p. 4, pp. 2(h).

³³⁰ Article 29 Data Protection Working Party, *op. cit.*, p. 7.

³³¹ 2014 EU-Canada PNR Agreement, *supra* note 12, ANNEX, Passenger Name Record data elements referred to in Article 2(b).

³³² 2006 PNR Agreement provided a list of 25 elements to be transmitted to CBSA. 2006 EU-Canada PNR Agreement, *supra* note 9, Attachment A, 'PNR Data Elements Required by CBSA from Air Carriers.

³³³ 2014 EU-Canada PNR Agreement, *op. cit.*

³³⁴ *Ibid.*

³³⁵ Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information

³³⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 169

³³⁷ Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Done in Brussels, 30 September 2013, pp. 29

Furthermore, as Advocate General Paolo Mengozzi points out some of those categories are formulated in a very excessively, open manner, without a reasonably informed person being able to determine either the nature or the scope of the personal data which those categories might contain, to be exact “available frequent flyer and benefit information (free tickets, upgrades, etc.)”; “all available contact information (including originator information)”, and heading of “general remarks”³³⁸. Even though Agreement provides that no other data must be communicated to the Canadian competent authority, since Canada is required to delete upon receipt any data transferred to it if it is not listed in the Annex to the Agreement³³⁹, in the light of unclear and imprecise heading it is particularly difficult to understand what data is to be regarded as not having to be transferred to Canada and therefore as having to be deleted by Canada.³⁴⁰

Moreover, 2006 EU-Canada PNR Agreement excluded sensitive data³⁴¹, which is not the case with 2014 EU-Canada PNR Agreements. According to the 2014 EU-Canada PNR Agreement Canadian Competent Authority shall “mask” sensitive data using automated systems.³⁴² Agreement provides safeguards for processing of sensitive data. Although sensitive data must be deleted after maximum retention period of 15 days and processed only on a case-by-case basis under strict procedural measures in “[...] exceptional circumstances where such processing is indispensable because an individual’s life is in peril or there is a risk of serious injury”³⁴³ under previous recommendations sensitive data has to be completely excluded from processing.³⁴⁴ The provision governing deletion of sensitive data permits the retention period to be no longer than 15 days from the date that Canada receives it. However, the Agreement provides PNR data retention if it is “required for any specific action, review, investigation, enforcement action, judicial proceeding, prosecution, or enforcement of penalties, until concluded”³⁴⁵. This implies, in the words of Advocate General Paolo Mengozzi, that sensitive data of a Union citizen who has taken a flight to Canada is

³³⁸ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 217

³³⁹ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 4(3)

³⁴⁰ Opinion 1/15 of Advocate General Paolo Mengozzi, *op. cit.*, pp. 219

³⁴¹ 2006 EU-Canada PNR Agreement, *supra* note 9, pp. 4.

³⁴² 2014 EU-Canada PNR Agreement, *op. cit.*, pp.8(1).

³⁴³ *Ibid.*, pp.8(3-5).

³⁴⁴ The Article 29 Working Party Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries (WP 178), adopted on 12 November 2010 and the EDPS Opinion of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ C 35/03, 09.02.2012, p.16.

³⁴⁵ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 16(5).

liable to be retained for five years (and, where appropriate, unmasked and analyzed during that period) by any Canadian public authority, for any ‘action’ or ‘investigation’ or ‘judicial proceeding’, without being in any way connected to the objective pursued by the agreement.³⁴⁶ Therefore, this provision prompts the conclusion that on this point 2014 EU-Canada Agreement has not struck a fair balance between public security objectives pursued by the agreement therefore, exceeded the limits of what was appropriate and necessary, to be exact, proportional to attain this public security objective and is incompatible with Articles 7, 8 and 52(1) of the Charter.

The comparison between the different EU-USA PNR Agreements with regard to the amount of data sets does not reveal any progress. The 2007 EU-USA PNR Agreement seemed to reduce the amount of elements to be transferred³⁴⁷, however, in reality, the same data sets have been summarized under fewer points than in the 2004 EU-USA PNR Agreement³⁴⁸. This is also the case with 2012 EU-USA PNR Agreement. The 2012 EU-USA Agreement maintains³⁴⁹ the same 19 data categories as the 2007 EU-USA PNR Agreement. It has to be observed that the list provided by 2012 EU-USA PNR Agreement is identical to the list introduced by 2014 EU-Canada PNR Agreement. This means that observations made while assessing the 2014 EU-Canada Agreement concerning data elements to be collected apply exactly the same to 2012 EU-USA PNR Agreement. Under 2012 EU-USA PNR Agreement the list of data elements consists of rather widely presented data elements such as “all available contact information”, “all baggage information” and “general remarks” which was excluded under its predecessor.³⁵⁰ As it was observed under the 2014 EU-Canada PNR Agreement “general remarks” such as OSI, SSI and SSR information, for instance, eating preference, special dietary requirements or special request for a wheelchair may reveal data related to ethnic origin, religious beliefs or health. That is to say, aforementioned PNR data apt to contain such sensitive data which should be explicitly excluded³⁵¹. Therefore, 2012 EU-USA PNR Agreement goes beyond what is strictly necessary by including in its scope the transfer of PNR data that is apt to contain sensitive data, which in material terms allows information about the health or

³⁴⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 224

³⁴⁷ 2007 EU-USA PNR Agreement, *supra* note 69, ANNEX US letter to EU, Title III, 2007 PNR Agreements cites only 19 elements grouped into sets of information.

³⁴⁸ Annex to Decision 2004/535/EC of 14 May 2004, *supra* note 231, Attachment “A” PNR Data Elements Required by CBP from Air Carriers, it was provided that such list encompasses 34 elements.

³⁴⁹ 2012 EU-USA PNR Agreement, *supra* note 11, ANNEX, PNR data types, it provides the list of 19 elements.

³⁵⁰ 2012 EU-USA PNR Agreement, *supra* note 11, ANNEX, PNR data types.

³⁵¹ Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union, *supra* note 255, pp. 29

ethnic origin or religious beliefs of the passenger concerned and and/or of those travelling with him to be disclosed. Thus, is incompatible with Articles 7, 8 and 52(1) of the Charter.

Moreover, some of the categories listed in the 2012 EU-USA PNR Agreement as it was replicated in 2014 EU-Canada PNR Agreement seems to be formulated in a very excessively, open manner, without being able to determine either the nature or the scope of the personal data which those categories might contain, in particular, “available frequent flyer and benefit information (free tickets, upgrades, etc.)”, “all available contact information (including originator information)”, and heading of “general remarks”³⁵². Since US is obliged to delete upon receipt any data transferred to it if it goes beyond those listed in the Annex to the Agreement³⁵³ it is rather important to understand the nature and the scope of these categories in order to determine what data is to be regarded as having to be deleted by US. In the light of unclear and imprecise heading of the aforementioned categories it may be particularly difficult to understand what data is to be deleted by US.

As regards sensitive data, the 2004 EU-USA PNR Agreement stated that CBP would not use this type of information and would implement, with the least possible delay, an automated system, which filters and deletes it.³⁵⁴ Both safeguards were watered down in 2007 EU-USA PNR Agreement, where the automated filtering did not require immediate deleting of the data and the use of such data was admitted in exceptional case where the life of a data subject or of others could be imperiled or seriously impaired.³⁵⁵ In such a case, “[...] the data was to be deleted within 30 days once the purpose for which it has been accessed is accomplished unless the further retention was required by law”³⁵⁶. The 2012 EU-USA PNR Agreement obliges DHS to employ automated systems to filter and mask out sensitive data from PNR”³⁵⁷. However access to, as well as processing and use of, sensitive data is still permitted in exceptional circumstances “[...] where the life of an individual could be imperiled or seriously impaired”³⁵⁸ which is the case anyhow connected to the purpose of

³⁵²2012 EU-USA PNR Agreement, op. cit.

³⁵³ Ibid., pp. 3.

³⁵⁴ Paragraph 9 et seq. of the Undertakings of the 2004 Agreement, supra note 233.

³⁵⁵ Paragraph III of the US letter to the EU,

³⁵⁶ Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security”, supra note 206, pp.3.4

³⁵⁷ 2012 EU-USA PNR Agreement, supra note 11, pp. 6(1, 3).

³⁵⁸Ibid., pp. 6(1,3).

the Agreement. As a result, the amount of information that US authorities can obtain and process has become very wide and it is not proportionate to the aims pursued by the Agreement.

If the 2012 EU-USA PNR Agreement provides the deletion of sensitive data after “[...] 30 days from the last receipt of PNR containing such data by DHS”, in that case, as Prof. Dr. Gerrit Hornung, Dr. Franziska Boehm observes, sensitive data of passengers flying again within 30 days will be retained for an additional 30 days from the second flight, and in the case of frequent travelers, the data may not be deleted at all, without any further requirement.³⁵⁹

Notwithstanding that, sensitive data may be retained even longer “[...] for the time specified in US law for the purpose of a specific investigation, prosecution or enforcement action”³⁶⁰. This may be interpreted as to considerably broadening the use of sensitive data. This provision makes no reference to the time period of retention of that data and purpose limitation of that agreement. This implies that sensitive data of a Union citizen who has taken a flight to USA is liable to be retained by USA for unknown period of time specified in the US law for any “investigation”, “prosecution” or “enforcement action”, without it being in any way connected to the public security objective pursued by the agreement. This prompts the conclusion that 2012 EU- USA PNR Agreement has not struck a fair balance between the public security and fundamental rights to privacy and data protection. Particularly because in cases of frequent travelers the data may not be deleted at all as well as “sensitive data” is liable to be retained by USA for an unknown period of time for any “investigation”, “prosecution” or “enforcement action” without being in any way connected to the public security objective. It follows that the use of sensitive data provided by the 2012 EU-USA PNR Agreement is incompatible with Articles 7 and 8 and Article 52(1) of the Charter.

As regards EU-sourced data elements to be collected, 2012 EU-Australia PNR Agreement as its predecessor provides an identical list of 19 elements³⁶¹ the only difference being that the latest Agreement holds the provision which entitles Australia not to require air carriers to provide data elements which are not already collected or held in their reservation systems and delete data which

³⁵⁹ Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security”, op. cit., pp.3.4.

³⁶⁰ 2012 EU-USA PNR Agreement, op. cit., pp. 6(4).

³⁶¹ 2012 EU-Australia PNR Agreement, supra note 11, p. 4, ANNEX 1.

include data beyond those listed in the Annex.³⁶² Even so, 2012 EU-Australia Agreement holds the exact same list of data elements to be collected as 2014 EU-Canada and 2012 EU-USA PNR Agreements. Although 2008 EU-Australia Agreement along with 2012 EU-USA and 2014 EU-Canada PNR Agreements were severely criticized as being excessive and disproportionate for holding “open text” such as “all available contact information”, “all baggage information” and “general remarks” in their PNR data lists, 2012 EU-Australia PNR Agreement consists of the identical elements³⁶³. As it was observed before, “general remarks” such as OSI, SSI and SSR information, may reveal data related to ethnic origin religious beliefs or health. Therefore this PNR data may contain such sensitive data which should be explicitly excluded.

The same criticism can be applied to some categories of PNR data which are formulated in a very excessively, open manner without being able to determine either the nature or the scope of the personal data those categories might contain. In particular, “available frequent flyer and benefit information (free tickets, upgrades, etc.)”, “all available contact information (including originator information)”, and heading of “general remarks” should be considered as such. As noticed by European Data Protection Supervisor the presence of open data fields could undermine legal certainty, therefore those categories should be better defined.³⁶⁴ Australia has an obligation to delete transferred data if it goes beyond those listed in the listed in the Annex to the Agreement³⁶⁵. However, it may be particularly difficult to determine what data is to be deleted if unclear and imprecise heading are provided by the Agreement.

What is relatively new under 2012 EU-Australia PNR Agreement is that it still holds its predecessors’ attitude towards exclusion of any further processing of sensitive data³⁶⁶. In any event, sensitive data elements are to be deleted immediately³⁶⁷ which was not the case under both 2012 EU-USA and 2014 EU-Canada PNR Agreements. Although sensitive data is deleted immediately, some categories, to be exact, “general remarks” are still able to reveal sensitive data. Therefore, 2012 EU-Australia Agreement goes beyond what is strictly necessary by including in its scope the

³⁶² 2012 EU-Australia PNR Agreement, *ibid.*, pp. 4(2-3)

³⁶³ *Ibid.*, p. 4, ANNEX 1.

³⁶⁴ Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Done in Brussels, 9 December 2011, pp. 5.

³⁶⁵ 2012 EU-Australia PNR Agreement, *supra* note 11, p. 4, ANNEX 1.

³⁶⁶ 2008 EU-Australia PNR Agreement, *supra* note 10, ANNEX, pp. 10.

³⁶⁷ 2012 EU-Australia PNR Agreement, p. 4, pp. 8.

transfer of PNR data that is apt to contain sensitive data, which in material terms allows information about the health or ethnic origin or religious beliefs of the passenger. Thus, is proportional and incompatible with Articles 7 and 8 and Article 52(1) of the Charter.

Summing up the analysis of the data elements to be collected of all PNR Agreements, one must conclude that the deficiencies pertinent to all the PNR agreements may be identified. In order to ensure the legal security of passengers, the categories of data in the Annexes to the Agreements should be drafted in a more concise and more precise manner, without any discretion being left to either the air carriers or the competent authorities as regards the actual scope of those categories to understand what data is to be regarded as having to be deleted by those authorities. Furthermore, all the PNR Agreements go beyond what is strictly necessary by including in their scope the transfer of PNR data that is apt to contain sensitive data, which in material terms allows information about the health or ethnic origin or religious beliefs of the passenger concerned which has to be explicitly excluded. Thus, are incompatible with Articles 7, 8 and 52(1) of the Charter. Further processing of sensitive data is excluded under 2012 EU-Australia PNR agreement. However, the 2014 EU-Canada PNR Agreement implies that sensitive data of a Union citizen who has taken a flight to Canada is liable to be retained for five years (by any Canadian public authority, for any ‘action’ or ‘investigation’ or ‘judicial proceeding’, without being in any way connected to the public security objective pursued by the agreement. Therefore, this provision prompts the conclusion that on this point 2014 EU-Canada Agreement exceeded the limits of what was appropriate and necessary to attain this objective and is incompatible with Articles 7, 8 and 52(1) of the Charter. In this sense, the 2012 EU- USA PNR Agreement has not struck a fair balance between the public security and fundamental rights to privacy and data protection either. Particularly because as Prof. Dr. Gerrit Hornung, Dr. Franziska Boehm observes, sensitive data of passengers flying again within 30 days will be retained for an additional 30 days from the second flight, and in the case of frequent travelers, the data may not be deleted at all as well as “sensitive data” is liable to be retained by USA for an unknown period of time for any “investigation”, “prosecution” or “enforcement action” without being in any way connected to the public security objective. It follows that the use of sensitive data provided by the 2012 EU-USA PNR Agreement is incompatible with Articles 7 and 8 and Article 52(1) of the Charter.

3.2.3. Proportionality of the data retention periods ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements

In order to be proportional personal data should be kept for no longer than it is necessary for the purposes for which they were collected. It should be reduced to minimum and, at the same time, long enough to carry out all necessary procedures. Even more, according to the Arr. 29 WP it is doubtful whether an excessively long data retention time with regard to millions of individuals can be effective for investigative purposes.³⁶⁸ Thus, only retention of the transferred data in line with the announced purpose may be accepted.³⁶⁹ Furthermore, data should only be retained for a short period that should not exceed some weeks or even months following the entry to the territory of a particular country. Indeed, according to the Art. 29 WP a short period of retention would seem better adopted to solve the highly difficult tasks.³⁷⁰ However, this is obviously without prejudice to “[...] the possible need for the processing to continue on a transitional basis in individual cases where there are well-established, specific grounds to examine certain persons more closely, in view of taking measures related to their actual and/or potential involvement in terrorist activities”³⁷¹.

As regards data retention periods, 2014 EU-Canada PNR Agreement provides five (5) years of the maximum period of data retention from the initial receipt of the data³⁷². The new 2014 EU-Canada PNR Agreement clearly rejected the two-periods of data retention established under its predecessor which divided time period according to a fact if a person is the subject of an investigation in Canada or not³⁷³. The retention period has been extended by one and a half (1,5) years by comparison with the period provided for in the 2006 Agreement, which was three and a half (3,5) years. As Dr. Michele Nino notices, this term under 2006 EU-Canada PNR Agreement seemed to be in compliance with the proportionality and data quality principles provided for by

³⁶⁸ Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data*, supra note 324, p. 8.

³⁶⁹ Article 29 Data Protection Working Party, *ibid.* p. 8.

³⁷⁰ *Ibid.* p. 8.

³⁷¹ Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data*, supra note 324, p. 8.

³⁷² 2014 EU-Canada PNR Agreement, supra note 12, pp.16(1)

³⁷³ 2006 EU-Canada PNR Agreement, supra note 9, pp. 8, 9. Where PNR information relates to a person who is not the subject of an investigation in Canada it will be retained in the PAXIS system for a maximum of 3.5 years. Where PNR information relates to a person who is the subject of an investigation in Canada it will be retained in that system for no longer than is necessary, and in any case for a period of no more than six years, at which time it will be destroyed unless it is required to be retained for an additional period.

Community law.³⁷⁴ However, 2014 EU-Canada PNR Agreement does not indicate the objective reasons that led the contracting parties to increase the PNR data retention period to a maximum of five (5) years.³⁷⁵ In the view of Advocate General Paolo Mengozzi, these objective reasons must be stated in the agreement, thus ensuring at the outset that this period is necessary for the objectives pursued by the Agreement.³⁷⁶

Notwithstanding five (5) year period, in cases, required for any specific action, review, investigation, enforcement action, judicial proceeding, prosecution, or enforcement of penalties PNR data may be retained until these cases are concluded.³⁷⁷ Aforementioned data may be retained for additional period of two (2) years to ensure the accountability of or oversee public administration so that it may be disclosed to the passenger if the passenger requests it³⁷⁸. Advocate General Paolo Mengozzi underlines, that the scope of aforementioned provisions should be confined to the purpose limitation thus providing objective reasons in the Agreement to ensure that maximum period of retention for five years is necessary.³⁷⁹

Furthermore, Canada depersonalizes the PNR data through masking the names of all passengers thirty (30) days after Canada receives it and further depersonalizes it through masking certain categories³⁸⁰ two (2) years after Canada receives the PNR data.³⁸¹ Even though EDPS has expressed concerns about the period during which the data will be available before being "further depersonalized" and recommended anonymising the data immediately after analysis and 30 days after reception as a maximum. ³⁸² It also states that the PNR data in certain categories³⁸³ listed in

³⁷⁴ Nino, M., "The protection of personal data in the fight against terrorism", supra note 20, p. 78

³⁷⁵ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 279

³⁷⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *ibid.*, pp. 280

³⁷⁷ 2014 EU-Canada PNR Agreement, *op. cit.* pp.16(5)(a)).

³⁷⁸ 2014 EU-Canada PNR Agreement, *ibid.*, pp.16(5)(b)).

³⁷⁹ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 280.

³⁸⁰ 2014 EU-Canada PNR Agreement, supra note 12, pp. 16(3)

(a) other names on PNR, including number of travelers on PNR;

(b) all available contact information (including originator information);

(c) general remarks including other supplementary information (OSI), special service information (SSI) and special service request (SSR) information, to the extent that it contains any information capable of identifying a natural person; and

(d) any advance passenger information (API) data collected for reservation purposes to the extent that it contains any information capable of identifying a natural person;

³⁸¹ 2014 EU-Canada PNR Agreement, *op. cit.*, pp. 16(3)

³⁸² Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Done in Brussels, 30 September 2013, p.6

³⁸³ 2014 EU-Canada PNR Agreement, *op. cit.*, pp. 16(3).

the Annex to the Agreement is to be masked two (2) years after it is received if, in the case of the last two categories, it is capable of identifying a natural person.³⁸⁴ However, it has to be observed that other headings in the Annex to the Agreement are also capable of directly identifying a natural person but do not appear on the list.³⁸⁵ For instance, “the available frequent flyer and benefit information” and/or “all available payment/billing information” which may include details of the payment method or methods used. Therefore, in the opinion of Advocate General Paolo Mengozzi, by omitting to ensure the ‘depersonalisation’ by masking of all the PNR data on the basis of which a passenger may be indirectly identified, the contracting parties have not struck a fair balance between the public security objective pursued by the Agreement.³⁸⁶

As regards the rules and procedures applicable to the unmasking of the PNR data³⁸⁷, Agreement states that such an operation can be carried out only if on the basis of available information it is necessary to carry out investigations under the scope of purpose limitation of the agreement either, up to two (2) years from initial receipt of the PNR data, by a limited number of specifically authorised officials or, between two (2) years and five (5) years after receipt, only with prior permission by the Head of the Canadian Competent Authority (hereinafter Head) or a senior official specifically mandated by the Head³⁸⁸. However, these specially authorised officials to access unmasked PNR data are not provided. Furthermore, Canada is obliged to destroy the PNR data at the end of the PNR data retention period ³⁸⁹even though EDPS recommended deleting or anonymising (irreversibly) the data immediately after analysis and 30 days after reception as a maximum.³⁹⁰

(a) other names on PNR, including number of travelers on PNR;

(b) all available contact information (including originator information);

(c) general remarks including other supplementary information (OSI), special service information (SSI) and special service request (SSR) information, to the extent that it contains any information capable of identifying a natural person; and

(d) any advance passenger information (API) data collected for reservation purposes to the extent that it contains any information capable of identifying a natural person;

³⁸⁴ Opinion 1/15 of Advocate General Paolo Mengozzi, *op. cit.*, pp. 286

³⁸⁵ 2014 EU-Canada PNR Agreement, *supra* note 12, ANNEX, Passenger Name Record data elements referred to in Article 2(b), pp. 5,8.

³⁸⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 287

³⁸⁷ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 16(4)

³⁸⁸ 2014 EU-Canada PNR Agreement, *ibid.*, pp. 16(4)(a)(b).

³⁸⁹ 2014 EU-Canada PNR Agreement, *ibid.*, pp. 16(6).

³⁹⁰ Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada, *supra* note 282, p.6

Advocate General Paolo Mengozzi observes that the contracting parties have not shown that it is necessary to retain all the PNR data for a maximum period of five years.³⁹¹ In his opinion, as regards the amount of PNR data retained, it is worth asking whether, after several years, there is justification for retaining certain categories of PNR data, since the Canadian competent authority has or may have it at its disposal, by means of unmasking in accordance with the conditions laid down above, the PNR data revealing the essential information relates to the identity of the passenger or passengers on PNR, the date of travel, the payment methods used, all available information, the travel itinerary, details of the travel agency or travel agent and baggage information.³⁹² In particular, whether frequent flyer and benefit information³⁹³, information about the check-in status of the passenger³⁹⁴, ticketing or ticket price information³⁹⁵ and code sharing information³⁹⁶ which provide information only about the actual carrier prove, after being retained for some years, will be information having genuine added value by comparison with the other PNR data which is also retained and which may be unmasked, with the aim of combating terrorism and serious transnational crime.³⁹⁷

When comparing EU-US PNR Agreements, a noticeable extension regarding the retention period can be observed. Whereas in the 2004 EU-US PNR Agreement the retention period was limited to three and a half (3.5) years (additional eight (8) years of retention period only for the data which had been accessed during the first three and a half (3.5) years).³⁹⁸ The 2007 EU-USA PNR Agreement allowed data retention in an “active analytical database” for seven (7) years and additional eight (8) years in the “dormant, non-operational” status.³⁹⁹ As Dr. Michele Nino observes, retention period provided by 2007 EU-USA PNR Agreement was already viewed as disproportionate and excessive in relation to the purposes to be achieved.⁴⁰⁰ However, the 2012 PNR

³⁹¹ Opinion 1/15 of Advocate General Paolo Mengozzi, op. cit., pp. 281.

³⁹² Opinion 1/15 of Advocate General Paolo Mengozzi, op. cit., pp. 284.

³⁹³ 2014 EU-Canada PNR Agreement, ANNEX Passenger Name Record data elements referred to in Article 2(b) heading 5.

³⁹⁴ 2014 EU-Canada PNR Agreement, supra note 12, ANNEX Passenger Name Record data elements referred to in Article 2(b) heading 13.

³⁹⁵ Ibid., heading 14.

³⁹⁶ Ibid., heading 11.

³⁹⁷ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 284.

³⁹⁸ Paragraph 15 of the Undertakings of the 2004 agreement, , After 3.5 years, PNR data that has not been manually accessed during that period of time, will be destroyed

³⁹⁹ 2007 EU-USA PNR Agreement, US letter to EU, Title VII.

⁴⁰⁰ 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, p. 76

Agreement widens data retention period even more. As EDPS observes, maximum retention period of 15 years is clearly disproportionate, irrespective of whether the data are kept in “active” or “dormant” databases.⁴⁰¹

However, the 2012 PNR Agreement widens data retention period even more. According to 2012 EU-USA PNR Agreement the PNR data should stay in “active database for up to 5 years” whereby “after the initial six (6) months of this period, PNR shall be depersonalized and masked”⁴⁰². Even so, USA does not provide any compelling reasons in the Agreement to demonstrate that this prolonged period of retention is strictly necessary and appropriate to attain public security objective. Therefore, this excessive period of data retention cannot be considered proportional and justified in the light of Article 7, 8 and 52(1) of the Charter.

Furthermore, in comparison, 2014 EU-Canada PNR Agreement provides masking of name after thirty (30) days of initial receipt of data and further depersonalizes certain categories after two (2) years it receives data. However, the 2012 EU-USA PNR Agreement masks name and other categories⁴⁰³ which are capable of identifying natural person only after six (6) months. Thus, categories which have to be masked are identical to the categories provided under 2014 EU-Canada PNR Agreement. However, as it was recognised before other heading of PNR data collected in the Annex to the Agreement are also capable of directly identifying a natural person but do not appear on the list. Data elements such as “available frequent flyer and benefit information” and/or “all available payment/billing information”⁴⁰⁴ which may include details of the payment method or methods used can be regarded as being able to identify a natural person. Therefore, by omitting to ensure the ‘depersonalisation’ by masking of all the PNR data on the basis of which a passenger may be directly identified, the 2012 EU-USA PNR Agreement has not struck proportionality between the public security objective and right to privacy and data protection.

⁴⁰¹Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, *supra* note 364, p. 5.

⁴⁰² 2012 EU-USA PNR Agreement, *supra* note 11, pp. 8(1).

⁴⁰³ 2012 EU-USA PNR Agreement, *supra* note 11., pp. 8(2):

- (a) name(s);
- (b) other names on PNR;
- (c) all available contact information (including originator information);
- (d) general remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and
- (e) any collected Advance Passenger Information System (APIS) information.

⁴⁰⁴ *Ibid.*, Annex, PNR DATA TYPES, pp. 5,7.

After five (5) years, the PNR are “transferred to a dormant database for a period of up to ten years”⁴⁰⁵. The wording “up to ten (10) years” does not give an impression of specifically limited period of retention time it rather implies that data can be retained even longer. In the dormant database, the data can be “repersonalized” in “connection with law enforcement operations” in conjunction with “an identifiable case, threat or risk”⁴⁰⁶. Even though the EDPS strongly emphasized that the PNR data should therefore be anonymised (irreversibly) or deleted immediately after analysis or after a maximum of 6 months.⁴⁰⁷ Notwithstanding that, data which is related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived⁴⁰⁸. The scope of this provision should be confined to the purpose described under purpose limitation stating objective reasons in the Agreement to ensure that this period is necessary.

Finally, it is unclear and not convincing why 2012 EU-USA PNR Agreement⁴⁰⁹ singles out ten (10) year dormant period of retention as subject for specific evaluation.⁴¹⁰ Moreover, following the dormant period, the data are not to be deleted, but “fully anonymized” without the possibility of repersonalization⁴¹¹ which is again denied by the fact that it is possible to repersonalize data in connection with law enforcement operations. However, this provision does not make clear reference that these operations have to be necessarily carried out under the scope of purpose limitation of the Agreement. As regards PNR data collected for the purposes of transnational crimes that are punishable by a sentence of three (3) years or more in this dormant database may only be repersonalized for a period of up to five (5) years.⁴¹² Nonetheless, provisions governing the data retention in the dormant database do not specify procedures regarding “additional controls,

⁴⁰⁵ 2012 EU-USA PNR Agreement, op. cit. pp. 8(3).

⁴⁰⁶ 2012 EU-USA PNR Agreement, ibid, pp. 8(3).

⁴⁰⁷ Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, supra note 364, p. 5.

⁴⁰⁸ 2012 EU-USA PNR Agreement, supra note 11, pp. 8(5).

⁴⁰⁹ Ibid. pp. 8(6)

⁴¹⁰ Opinion of the Article 29 Working Party, (2012)15841 - 06/01/2012, pp. 8. < http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf> [last accessed 12-27-2016].

⁴¹¹ 2012 EU-USA PNR Agreement, op. cit., pp. 8(4).

⁴¹² Ibid., pp. 8(3).

including a more restricted number of authorised personnel, as well as a higher level of supervisory approval required before access”⁴¹³.

Furthermore, it must be observed that 2012 EU-USA PNR Agreement does not provide clear explanation of a need to retain all the PNR data for a maximum period of 15 years. The substantively changing form of elimination of data after the retention period has been expired vary from “destruction”⁴¹⁴ under the 2004 EU-USA PNR Agreement, “deletion”⁴¹⁵ under the 2007 EU-USA PNR Agreement and respectively to “anonymisation”⁴¹⁶ in 2012 EU-USA PNR Agreement reduces the protection of data and right to privacy of the data subjects. Even though, EU-USA Agreements were highly criticized for exceeding what is strictly necessary and appropriate for performance of the defined tasks⁴¹⁷, the growing expansion of data retention period by the 2012 EU-USA PNR Agreement indeed abolished the time limit entirely.

2012 EU-Australia PNR Agreement provides that Australian Customs and Border Protection Service shall retain PNR data no longer than five-and-a-half (5.5) years from the initial receipt and during this period PNR data shall be retained only for the purposes and ends of the Agreement.⁴¹⁸ While comparing this retention period with the previous 2008 EU-Australian PNR scheme it can be seen that the 2008 EU-Australia provided a data retention period of three-and-a-half (3.5) years and did not foresee the storage of data except on a case by case basis for investigation purposes.⁴¹⁹ However, in any case retention period under 2008 EU-Australia PNR Agreement did not exceed more than five-and-a-half (5.5) years after the date of receipt of the PNR data by Customs.⁴²⁰ 2012 EU-Australia PNR Agreement provides five-and-a-half (5.5) years data retention period including three (3) years without any masking of data. However, the 2012 EU-Australia PNR agreement itself does not show that it is necessary to retain all the PNR data for a maximum period of five and a half (5.5) years. The EDPS considers the length of the data retention period foreseen in 2012 EU-USA PNR Agreement as one of the major difficulties in the agreement. A period of retention of five and a

⁴¹³ Ibid., pp. 8(3).

⁴¹⁴ Paragraph 15 of the Undertakings of the 2004 agreement, supra note 233.

⁴¹⁵ 2007 EU-USA PNR Agreement, supra note 69, US letter to EU, Title VII.

⁴¹⁶ 2012 EU-USA PNR Agreement, supra note 11, pp. 8(4).

⁴¹⁷ Article 29 Data Protection Working Party, *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data*, supra note 324, p. 8.

⁴¹⁸ 2012 EU-Australia PNR Agreement, supra note 11, p. 4, pp. 16(1)

⁴¹⁹ Ibid, pp. 12

⁴²⁰ Ibid., pp. 12

half years, including three years without any masking of data, is clearly disproportionate, especially if this retention period is compared with the previous Australian PNR scheme, which did not foresee the storage of data except on a case-by-case basis.⁴²¹

Australian retention period is similar to the Canadian retention period of five (5) years and still rather short then compared to the 2012 EU-USA PNR Agreement which allows comprehensive retention period of fifteen (15) years. Although under 2012 EU-Australia PNR Agreement during the first three (3) years, the received data can only be accessible to a limited number of specifically authorised Australian Customs and Border Protection Service officials only after this period PNR data elements⁴²² that might lead to passengers being identified shall be masked out.⁴²³ However, it has to be observed again that other PNR data may also be capable of identifying a natural person but do not appear in this list. Particularly, worrying headings appear to be “available frequent flyer and benefit information” and/ or “all available payment/billing information” which may include details of the payment method or methods used.⁴²⁴ Therefore, by omitting to ensure the “depersonalisation” by masking all the PNR data which may directly identify a natural person, the 2012 EU-Australia PNR agreement has not struck proportional balance between public security and the right to privacy and personal data.

As regards PNR data retention required for a specific investigation, prosecution or enforcement of penalties 2012 EU-Australia PNR Agreement provides reference to the purposes of the Agreement, that is to say, PNR data retained for terrorist offences or serious transnational crime may be processed for the purpose of that investigation, prosecution or enforcement of penalties.⁴²⁵ Therefore, PNR data may be retained until the relevant investigation or prosecution is concluded or the penalty enforced. Eventually, upon the expiry of the data retention period, even the data that has

⁴²¹ Opinion of the European Data Protection Supervisor on the proposal for a Council decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service OJ C 322, 5.11.2011, pp. 30.

⁴²² 2012 EU-Australia PNR Agreement, supra note 11, pp. 16(2), *ANNEX I* (a) name(s);

(b) other names on PNR, including number of travelers on PNR;

(c) all available contact information (including originator information);

(d) general remarks including other supplementary information (OSI), special service information (SSI) and special service request (SSR) information, to the extent that it contains any information capable of identifying a natural person; and

(e) any collected advance passenger processing (APP) or advance passenger information (API) data to the extent that it contains any information capable of identifying a natural person.

⁴²³ 2012 EU-Australia PNR Agreement, op. cit., p. 4, pp. 16(2)

⁴²⁴ Ibid., *ANNEX*, pp. 5, 8.

⁴²⁵ 2012 EU-Australia PNR Agreement, op. cit., pp. 16(3)

been retained for a specific investigation, prosecution or enforcement of penalties has to be permanently deleted.⁴²⁶ Similar provisions are not found in other PNR Agreements. What is even more surprising that 2012 EU-Australia Agreement does not provide in any case unmasking or repersonalization after data has been masked out.

After assessing retention periods of all PNR Agreements, it has to be observed that interference which is incompatible with Article 7, 8 and 52(1) and common to all the Agreements has been found. In particular, while omitting to ensure the ‘depersonalisation’ by masking of all the PNR data on the basis of which a passenger may be directly identified and not involving all the categories that are also capable of identifying a natural person the 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements have not struck proportionality between the legitimate desire to preserve public security and the equally fundamental rights to respect privacy and persona data of the individuals concerned. Furthermore, the excessive period of data retention for 15 years provide by the 2012 EU-USA PNR Agreement cannot be justified as appropriate and proportional to attain public security objective. Repersonalization under 2012 EU-USA PNR Agreement, which may take place “in connection” with law enforcement operations exceeds what proportional and strictly necessary to attain public security objective as well, therefore is incompatible with Article 7, 8 and 52(1) of the Charter. Particularly serious interference which cannot be justified as proportional appears in the provision regarding retention of data in the dormant database, where data are not to be deleted, but “fully anonymized”. This indicates that data stays in the databases for as long as USA foresees which clearly goes beyond what is strictly necessary. The 2012 EU-Australia PNR Agreement is incompatible with Article 7, 8 and 52(1) because masking out of PNR data only three (3) years after the initial receipt does not struck the fair balance between public security and the right to protect privacy and personal data.

Nonetheless, it must be observed that none of the Agreements have shown that it is necessary to retain all the PNR data for a maximum period of retention. In particular, whether frequent flyer and benefit information, information about the check-in status of the passenger, ticketing or ticket price information and code sharing information which provide information only about the actual carrier, after being retained for some years, will be information having genuine added value by comparison

⁴²⁶ Ibid., pp. 16(4)

with the other PNR data which is also retained with the aim of combating terrorism and serious transnational crime.

3.2.4. Proportionality of the disclosure of data ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements

The further step in assessing proportionality of the envisaged Agreements is revision of the provisions on the data disclosure. The 2014 EU-PNR, 2012 EU-USA and 2012 EU-Australia Agreements provide two types of data disclosure, in particular, internal disclosure to other government authorities and external disclosure to third countries. As regards internal disclosure “[...] PNR data should only be disclosed to other government authorities with powers in the fight against terrorism and serious transnational crime, and which afford the same protections as afforded by the recipient agency under the Agreement in accordance with an undertaking to the latter”⁴²⁷. As regards external disclosure “[...] the receiving third country should transfer this information to a competent authority of another third country only if the latter undertakes to treat the data with the same level of protection as set out in the agreement and the transfer is strictly limited to the purposes of the original transfer of the data”⁴²⁸. In both cases PNR data should never be disclosed in bulk but only on a case-by-case basis.⁴²⁹

As for the disclosure of EU sourced PNR information, 2014 EU-Canada PNR Agreement provides two Articles 18 and 19 relating respectively to internal disclosure of PNR data by Canadian competent authorities to other Canadian government institutions and external disclosure to other government authorities of countries other than Member States of the EU. It can be seen from the Agreement that, there is no specification to which “other government authorities in Canada” the data may be disclosed.⁴³⁰ 2006 EU-Canada PNR Agreement did not specify those “other government authorities” either. Even more 2014 EU-Canada PNR Agreements maintains almost identical provisions concerning internal and external disclosure as its predecessor.⁴³¹

⁴²⁷ Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, *supra* note 127, p. 10.

⁴²⁸ *Ibid.*, p. 10.

⁴²⁹ *Ibid.*, p. 10.

⁴³⁰ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 18.

⁴³¹ 2008 EU-Canada PNR Agreement, *supra* note 9, pp. 16-20.

Articles 18 and 19 of the 2014 EU-Canada PNR Agreement make the subsequent transfer of PNR data or the analytical information containing PNR data subject to strict cumulative conditions, four of which are identical.⁴³² Thus, that data and that information are disclosed only if the government authorities have functions directly related to the scope of the purpose limitation of the agreement⁴³³, on a case-by-case basis⁴³⁴ and under the particular circumstances the disclosure is necessary for the purposes set under purpose limitation⁴³⁵. In addition, only the minimum amount of PNR data or analytical information necessary is to be disclosed.⁴³⁶

However, guarantees afforded by those two terms of the agreement differ from the other conditions. According to provision on internal disclosure, other Canadian government authorities to whom the PNR data is disclosed must afford “protection equivalent to the safeguards described in the Agreement”⁴³⁷. As regards external disclosure under 2006 EU-Canada PNR Agreement PNR information retained in PAXIS will be shared only with a country that has received an adequacy finding under the Data Protection Directive, or is covered by it.⁴³⁸ While provisions under 2014 EU-Canada PNR Agreement on external disclosure states⁴³⁹ that the Canadian Competent Authority must be “satisfied” that the foreign authority receiving the PNR data applies either standards to protect the PNR data that are equivalent to those set out in the Agreement⁴⁴⁰ or the standards to protect the PNR data that it has agreed with the Union.

It has to be observed that in both situations discretion to ascertain the adequacy of the protection afforded by the public authority receiving the data is left to the Canadian competent authority, in particular CBSA. Therefore, “neither the CBSA’s examination nor any decision on disclosure of the PNR data is subject to *ex ante* control by an independent authority or a judge”⁴⁴¹. Nor does the 2014 EU-Canada PNR Agreement provide that the “intention to transfer the EU national PNR data is at least to be notified to the competent authorities of the Member State in

⁴³² Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 297.

⁴³³ 2014 EU-Canada PNR Agreement, *op. cit.* pp. 18(1a), 19(1a).

⁴³⁴ *Ibid.*, pp. 18(1b), 19(1b).

⁴³⁵ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 18(1c), 19(1c).

⁴³⁶ *Ibid.*, pp. 18(1d), 19(1d).

⁴³⁷ *Ibid.*, pp. 18(1e).

⁴³⁸ 2008 EU-Canada PNR Agreements, pp. 18.

⁴³⁹ 2014 EU-Canada PNR Agreement, *op. cit.*, pp. 19(1e).

⁴⁴⁰ *Ibid.*, pp. 19(1e) In accordance with agreements and arrangements that incorporate those standards.

⁴⁴¹ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 297.

question and/or to the Commission before disclosure actually takes place”⁴⁴². Article 18 on internal disclosure of the Agreement is silent as to the latter possibility, while Article on external disclosure⁴⁴³ provides only that the competent authorities of the Member State in question are to be notified “at the earliest appropriate opportunity”. A mere “*post factum*” review of the disclosure of the data will not make it possible either to counterbalance an incorrect assessment of the level of protection afforded by a recipient public authority or to restore the privacy and confidentiality of the data when it has been transferred to and used by the recipient public authority.⁴⁴⁴ That is notably true in the case of the external disclosure of data to a third country, where its subsequent use will even be outside the *post factum* competence and review of the Canadian authorities and courts.⁴⁴⁵

Furthermore, as regards internal disclosure, receiving Canadian government authority is prohibited from subsequently disclosing the PNR data to another entity unless the disclosure is authorised by the CBSA respecting the conditions laid down in that paragraph.⁴⁴⁶ This safeguard is clearly missing in respect of external disclosure. In particular, the 2014 EU-Canada Agreement does not prohibit the receiving public authority of a third country from subsequently disclosing the PNR data to another entity as the case may be, to another third country before CBSA authorises this transfer.⁴⁴⁷ Therefore, as the risk that such a situation, which would have the effect of circumventing the level of protection of personal data afforded by EU law, may arise has not been excluded, it must be stated that provisions on external disclosure provided by the 2014 EU-Canada PNR Agreement authorizes unwarranted interferences with the fundamental rights guaranteed by Articles 7, 8 and 52(1) of the Charter. Thus exceeds what is proportional to preserve public security and equally fundamental right for everyone to enjoy a high level of protection of privacy and personal data, therefore is incompatible with the aforementioned guarantees.

As regards data disclosure, EU-USA PNR Agreements likewise entails internal PNR data disclosure to the domestic government authorities and external PNR data disclosure to third countries competent government authorities.⁴⁴⁸ With regard to internal disclosure of data under the 2004 PNR

⁴⁴² Ibid., pp. 300.

⁴⁴³ 2014 EU-Canada PNR Agreement, op. cit., pp. 19(2).

⁴⁴⁴ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 302

⁴⁴⁵ Ibid., pp. 302

⁴⁴⁶ 2014 EU-Canada PNR Agreement, supra note 12, pp. 18(1f).

⁴⁴⁷ Opinion 1/15 of Advocate General Paolo Mengozzi, op. cit., pp. 302

⁴⁴⁸ 2012 EU-USA PNR Agreement, supra note 11, pp. 16, 17.

Agreement, the CBP⁴⁴⁹ was permitted to disclose PNR data to other U.S. government authorities, however only to the authorities with counter terrorism or law enforcement functions on a case by case basis⁴⁵⁰. Further provisions permitted internal disclosure “[...] for the protection of the vital interests of the data subject or of other persons”⁴⁵¹ and “[...] the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law”⁴⁵². These wide ranging purposes for internal disclosure were further extended in the 2007 PNR Agreement regarding internal disclosure to authorities serving public security functions in support of “public security related cases (including threats, flights, individuals and routes of concern)”⁴⁵³. The 2012 EU-USA PNR Agreement permits internal disclosure of PNR data if it is exclusively consistent with purposes of preventing, detecting, investigating, and prosecuting terrorist offences and related crimes and other transnational crimes. Internal disclosure can be made only with domestic government authorities when acting in furtherance of the aforementioned purposes.⁴⁵⁴ However, as it was mentioned before, USA uses PNR data not only to those stated purposes but also for border security, the use of PNR if ordered by a court or other violations of law.⁴⁵⁵ As Prof. Dr. Gerrit Hornung, Dr. Franziska Boehm states, this could lead to the surplus of domestic authorities authorized to receive PNR⁴⁵⁶. Even though PNR data is obliged to be internally disclosed “only in support of those cases under examination or investigation”⁴⁵⁷ the 2012 EU-USA PNR agreements does not specify whether those cases have to be related to the terrorist offences and related crimes including other crimes that are punishable by a sentence of imprisonment of three (3) years or more and are transnational in nature.

The only substantive requirement as regards internal disclosure apart from being somehow related to these purposes appears to be that receiving country shall afford “[...] equivalent or comparable safeguards” as set out in the 2012 PNR Agreement, which has to be respected.⁴⁵⁸ However, it has to

⁴⁴⁹ The Department of Home Land Security Bureau of Customs and Border Protection (CBP) which is now a department of Department of Homeland Security (DHS and was the receiving partner at that time).

⁴⁵⁰ Paragraphs 28 et seq. of the Undertakings of the 2004 agreement, supra note 233.

⁴⁵¹ in particular regarding health risks

⁴⁵² Paragraphs 34 and 35 of the Undertakings of the 2004 agreement, supra note 233.

⁴⁵³ 2007 EU- USA PNR Agreement, supra note 9, Paragraph II of the US letter to the EU.

⁴⁵⁴ 2012 EU-USA PNR Agreement, supra note 12, pp. 16(1a-b).

⁴⁵⁵ Ibid., pp. 16(1a-b) and 4(3,4).

⁴⁵⁶ Hornung, G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security “, supra note 306, pp.3.3

⁴⁵⁷ 2012 EU-USA PNR Agreement, op. cit., pp. 16(1d).

⁴⁵⁸ Ibid., pp. 16(1c).

be observed that the discretion to ascertain the adequacy of the protection afforded by the public authority receiving the data is left to the US competent authority, in particular DHS.

Even so, it has also to be observed, that the 2012 EU-USA PNR Agreement concerning internal disclosure is clearly missing basic safeguards, which are provided by 2014 EU-Canada PNR Agreement. That is to say, PNR data may be internally disclosed to other government authorities if their functions are directly related to the scope of the purpose limitation, only on the case-by-case basis, only the minimum amount of PNR data necessary and if the receiving government authority does not disclose the PNR data to another entity unless the disclosure is authorized by the competent authority respecting the conditions laid down as regards internal disclosure. However, 2012 EU-USA PNR Agreement as regards internal disclosure of data fails to lay down substantive safeguards apart from receiving authority being somehow related to the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and related crimes, including other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature and being able to afford equivalent or comparable safeguards as set out in the Agreement. Therefore, provisions of the 2012 EU-USA PNR agreement regarding internal disclosure of PNR data are incompatible with Article 7, 8 and 52(1) of the Charter particularly because they do not provide any substantive safeguards to the PNR data which is why are not proportional to the desire to preserve public security and equally fundamental right to the protection of privacy and personal data.

As for the external disclosure, the 2004 EU-USA PNR Agreement as well as the 2007 EU-USA PNR Agreement, imposed that PNR data may only be provided to foreign government authorities with counter terrorism or law enforcement functions on a case by case basis⁴⁵⁹ as well as other purposes mentioned in the agreements including the protection of the vital interests of the data subject or other persons and the use in any criminal judicial proceeding⁴⁶⁰. A new clause was introduced in the 2007 EU-USA PNR Agreement, requiring that data exchanges should only be carried out, apart from emergency circumstances, if “express understandings” between the third party and the DHS “that incorporate data privacy protection comparable to” those applied to the PNR by DHS were concluded beforehand⁴⁶¹. The 2012 EU-USA PNR Agreement maintains this safeguard clause stating that apart from emergency circumstances, any external transfer of data shall

⁴⁵⁹ Paragraph 29 of the Undertakings of the 2004 agreement, *supra* note 233.

⁴⁶⁰ 2007 EU-USA PNR Agreement, *supra* note 69, Paragraph II, US letter to EU, annex to the 2007 agreement.

⁴⁶¹ *Ibid.*

occur pursuant to “express understandings” that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.⁴⁶²

However, provisions on external PNR disclosure in the 2012 EU-USA PNR Agreement appear to be very general and imprecise. In particular, it is stated that US may transfer PNR data to third countries competent authorities under terms consistent with the Agreement and only upon ascertaining the recipient’s intended use is consistent with those terms.⁴⁶³ It is clear from the aforementioned provision that the US is again left with the discretion to determine recipient’s consistency with the Agreement. Furthermore, PNR shall be disclosed only in support of those cases under examination or investigation.⁴⁶⁴ However, there is no reference to the particular purposes of the use of data therefore it may appear that PNR data can be externally disclosed under any examination or investigation. Therefore, generally presented provisions regarding external disclosure of PNR data are incompatible with Article 7, 8 and 52(1) of the Charter because they do not provide any substantive safeguards to the PNR data. Thus, does not preserve balance between the legitimate desire to preserve public security and the equally fundamental rights to the protection of private life and personal data.

Even though, 2012 EU-USA PNR Agreement introduces a new information duty this gives no added value as regards safeguards of external disclosure⁴⁶⁵. In particular, competent authorities of the concerned Member State must now be informed, if the PNR of an EU citizen or resident is transferred to a third country⁴⁶⁶. However, it has to be notified “[...] at the earliest appropriate opportunity” which was also a case introduced by the 2014 EU-Canada PNR Agreement. Therefore, as expressed by the Advocate General Paolo Mengozzi expressed a “*post factum*” review of the disclosure of the data will not make it possible either to counterbalance an incorrect assessment of the level of protection afforded by a recipient public authority or to restore the privacy and confidentiality of the data when it has been transferred to and used by the recipient public authority.⁴⁶⁷

⁴⁶² 2012 EU-USA PNR Agreement, supra note 11, pp. 17(2).

⁴⁶³ 2012 EU-USA PNR Agreement, supra note 11, pp. 17(1).

⁴⁶⁴ Ibid., pp. 17(1).

⁴⁶⁵ Ibid., pp. 17(2).

⁴⁶⁶ Ibid., pp. 17(4).

⁴⁶⁷ Opinion 1/15 of Advocate General Paolo Mengozzi, supra note 29, pp. 302

As regards internal disclosure, the 2012 EU-Australia PNR Agreement provides a clear list⁴⁶⁸ of government authorities with which PNR data may be shared, the list is a one organization wider comparing to its predecessor.⁴⁶⁹ It has to be observed that the 2012 EU-Australia PNR Agreement maintains almost identical provisions concerning internal and external disclosure as its predecessor.⁴⁷⁰ Articles 18 and 19 of the 2012 EU-Australia PNR Agreement make the subsequent transfer of PNR data or the analytical information containing PNR data subject to strict cumulative conditions, five of which are identical.

In particular, in order to obtain PNR data receiving government authorities whose functions are directly related to preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime shall afford to PNR data the safeguards as set out in the Agreement.⁴⁷¹ Furthermore, data shall be shared strictly for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime only on a case-by-case basis⁴⁷². In any case minimum amount of data shall be shared after assessing the necessity of that data.⁴⁷³ Furthermore, receiving government authorities shall ensure that the data is not further disclosed without the permission of the Australian Customs and Border Protection Service.⁴⁷⁴

In order to disclosure PNR data externally, the Australian Customs and Border Protection Service has to be satisfied that the receiving authority has agreed not to further transfer PNR data.⁴⁷⁵

⁴⁶⁸ 2012 EU-Australia PNR Agreement, *supra* note 11, pp. 18(1) and ANNEX 2. List of other government authorities of Australia with whom the Australian Customs and Border Protection Service is authorised to share PNR data:

1. Australian Crime Commission;
2. Australian Federal Police;
3. Australian Security Intelligence Organisation;
4. Commonwealth Director of Public Prosecutions;
5. Department of Immigration and Citizenship;
6. Office of Transport Security, Department of Infrastructure and Transport.

⁴⁶⁹ 2008 EU- Australia PNR Agreement, *supra* note 10, ANNEX 2,

List of other government authorities of Australia with whom the Australian Customs and Border Protection Service is authorised to share PNR data:

1. Australian Crime Commission;
2. Australian Federal Police;
3. Australian Security Intelligence Organisation;
4. Commonwealth Director of Public Prosecutions; and
5. Department of Immigration and Citizenship.

⁴⁷⁰ *Ibid.* ANNEX ,pp. 2-6.

⁴⁷¹ 2012 EU-Australia PNR Agreement, *supra* note 11, pp. 18(1a, 2b), 19(1a-b).

⁴⁷² *Ibid.* pp. 18(1b-c), 19(1c-d).

⁴⁷³ *Ibid.*, pp. 18(1d), 19(1e).

⁴⁷⁴ *Ibid.*, pp. 4, pp. 18(1e).

⁴⁷⁵ *Ibid.*, p. 4, pp. 19(1h).

This provision has never been introduced by the 2014 EU-Canada and 2012 EU-USA Agreements. Additionally, as regards external disclosure 2012 EU-Australia PNR Agreement foresees the duty to inform competent authorities of the Member States “[...] at the earliest appropriate opportunity” in cases where PNR data of national or resident of Member State is transferred.⁴⁷⁶ However, as it was considered before in the analysis of 2014 EU-Canada and 2012 EU-USA PNR Agreements, “post factum” review of the disclosure of the data will not make it possible to either restore the privacy and confidentiality of the data when it has been already transferred to and used by the recipient public authority or to counterbalance an incorrect assessment of the level of protection afforded by a recipient public authority.

Even more, the Australian Customs and Border Protection Service has a duty to ensure that the passenger is informed of a transfer of his or her PNR data to authorities of third countries.⁴⁷⁷ This provision seems to be a newly establish safeguard providing “a right to know” to a person concerned.

Furthermore, none of the other assessed PNR Agreements provided that in order to receive PNR data from the Australian Customs and Border Protection Service authority of a third country has to agree to retain PNR data only until the relevant investigation or prosecution is concluded or the penalty enforced or are no longer required for the protection of the vital interests of any individual, such as risk of death, serious injury or threat to health, and in any case no longer than necessary.⁴⁷⁸

After careful assessment of internal and external disclosure of PNR data under 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements, the following observations are made. Only 2012 EU-Australia PNR Agreement PNR provides clear and precise provisions which do not seem to be disproportional and are compatible with Article 7, 8 and 52(1) of the Charter. As regards external disclosure under 2014 EU-Canada Agreement it does not prohibit the receiving public authority of a third country itself to subsequently disclose PNR data to another entity as the case may be, to another third country before CBSA is satisfied about this transfer. Therefore, as the risk that such a situation may arise has not been excluded the 2014 EU-Canada PNR Agreement authorizes unwarranted interferences with the fundamental rights guaranteed by Articles 7, 8 and

⁴⁷⁶ 2012 EU-Australia PNR Agreement, *supra* note 11, p. 4, pp. 19(1)(f).

⁴⁷⁷ *Ibid.* pp. 19(1)(i).

⁴⁷⁸ *Ibid.* pp. 19(1)(g).

52(1) of the Charter. As regards internal and external disclosure of PNR data the 2012 EU-USA Agreement fails to lay down basic safeguards. In particular, apart from being somehow related to the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and related crimes, including other crimes that transnational in nature 2012 EU-USA PNR Agreement does not require receiving authority to provide any substantive safeguards to the PNR data. Therefore, this interference cannot be justified as being proportional to preserve public security in the light of Article 7, 8 and 52(1) of the Charter.

3.2.5. Proportionality of the guarantees for and rights of data subjects ascertained by 2014 EU-Canada, 2012 EU-USA and 2012 EU- Australia PNR Agreements

To assure adequate level of data protection regime the data subject, for instance, a person whose PNR data is processed, has to be provided with information about the transfer and processing of his personal data and to be able to exercise his/her rights, in an easy, quick and effective manner.⁴⁷⁹ Thus, data subjects should be clearly and precisely informed about their rights in particular about the right of access to his or her PNR data and the right to seek rectification and deletion of his or her PNR data in addition to the available redress effective mechanisms.⁴⁸⁰ Thus, every individual shall have the right to effective administrative and judicial redress where his or her privacy has been infringed or data protection rules have been violated, on a non-discriminatory basis regardless of nationality or place of residence.⁴⁸¹ Therefore, any such infringement or violation shall be subject to appropriate and effective sanctions and/or remedies.⁴⁸²

As regards information provided to the data subjects, 2014 EU-Canada Agreement states the contracting parties shall work with the air travel industry, to promote transparency, preferably at the time of booking, by providing the following information to passengers: the reasons for PNR data collection; the use of PNR data; the procedure for requesting access to PNR data; and the procedure for requesting the correction of PNR data.⁴⁸³ Furthermore, 2014 EU-Canada PNR Agreement

⁴⁷⁹Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, Adopted on 2 April 2003, 00569/13/EN WP 203, supra note 289, p. 4.

⁴⁸⁰ Ibid, p. 4.

⁴⁸¹ Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, supra note 127, p. 10

⁴⁸² Ibid., p. 10

⁴⁸³ 2014 EU-Canada PNR Agreement, supra note 12, pp. 11(2)

implies a duty on Canadian competent authority to provide certain information on its website, for instance, information regarding access, correction, notation and redress as well as contact information for inquiries.⁴⁸⁴

Regarding the access for individuals to their PNR data, 2014 EU-Canada PNR Agreement provides that Canada shall ensure that any individual may access their PNR data as well as may request the correction of their PNR data⁴⁸⁵. It was not a case in its predecessor. The 2006 EU-Canada PNR Agreement stated that according to Canadian law, persons who are not present in Canada cannot exercise the rights provided by the Canadian Privacy Act and the Access to Information Act.⁴⁸⁶ Therefore, the Memorandum D1-16-3 of the CBSA⁴⁸⁷ extended the rights of access, rectification, notation and redress to foreign nationals that are not present in Canada. Thus, any refusal to access PNR data or refusal of data correction has to be notified setting out the legal or factual reasons for any refusal to allow access to the individual's PNR data.⁴⁸⁸

However, certain limitations regarding legitimate interest of the individual concerned to seek access to PNR data can be made in order to prevent, detect, investigate, or prosecute criminal offences, or to protect public or national security.⁴⁸⁹ If PNR data is not a subject to reasonable legal requirements or limitations, this provision authorizes Canada to “make any disclosure of information [...], with due regard for the legitimate interests of the individual concerned”⁴⁹⁰. Nonetheless, as was precisely observed by Advocate General Paolo Mengozzi, neither the recipients of that “information” nor the use for which it may be requested is defined in the Agreement.⁴⁹¹ It has to be observed that it is rather possible that that information may be communicated to any natural or legal

⁴⁸⁴ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 11(1): Canada shall ensure that the Canadian Competent Authority makes the following available on its website:

(a) a list of the legislation authorizing the collection of PNR data;
(b) the reason for the collection of PNR data;
(c) the manner of protecting the PNR data;
(d) the manner and extent to which the PNR data may be disclosed;
(e) information regarding access, correction, notation and redress; and
(f) contact information for inquiries.

⁴⁸⁵ *Ibid.*, pp. 12(1), 13(1).

⁴⁸⁶ 2006 EU-Canada PNR Agreement, *supra* note 9, pp. 29

⁴⁸⁷ Canada Border Services Agency, Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data, Memorandum D1-16-3, Ottawa, May 31, 2016 ISSN 2369-2391, Superseded memorandum D1-16-3 dated January 14, 2010, pp. 39-40.

⁴⁸⁸ 2014 EU-Canada PNR Agreement, *op. cit.* pp. 12(2d), 13(2b)(ii)(i).

⁴⁸⁹ 2006 EU-Canada PNR Agreement, *op. cit.*, pp. 12(3)

⁴⁹⁰ 2014 EU-Canada PNR Agreement, *op. cit.*, pp. 12(3).

⁴⁹¹ Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 293

person, for instance a bank, “[...] providing that Canada considers that the disclosure of such information does not exceed “reasonable” legal requirements, which, moreover, are not defined in the agreement”⁴⁹². Thus, particularly vague nature of its wording and to the particularly broad terms in which it is couched⁴⁹³, provision governing “[...] any disclosure of information regarding the legitimate interests of the individual concerned access” seems to go beyond what is strictly necessary to attain the public security objective pursued by the Agreement. Therefore, this provision seems to be disproportional and incompatible with the Article 7, 8 and 52(1) of the Charter.

As for administrative and judicial redress, according to 2014 PNR Agreement any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek “[...] effective judicial redress or in accordance with Canadian law by way of judicial review, or such other remedy which may include compensation”⁴⁹⁴. Notwithstanding that, Canada provides internal autonomous oversight, that is to say, Canada shall “[...] ensure that an independent public authority, or an authority created by administrative means will receive, investigate and respond to complaints lodged by an individual concerning their request for access, correction or notation of their PNR data”.⁴⁹⁵ However, there is no reference in the Agreement to this competent authority. This raise question whether this authority enjoys complete independence and is competent to examine requests of that type. If independent supervisory authority would not be competent to examine requests of this kind or if this authority not fully enjoys independence from a political nature on the part of the authority to which it is responsible it cannot be regarded as an independent supervisory authority for the purposes of Article 8(3) of the Charter.⁴⁹⁶ The possibility that such a situation may arise, means that the contracting parties have not struck a fair balance between the objectives pursued by the Agreement therefore is incompatible with 7, 8 and 52(1) of the Charter.

As regard information to data subjects, 2012 EU-USA PNR Agreement implies a duty to DHS to publish its procedures and modalities regarding access, correction or rectification, and redress

⁴⁹² Opinion 1/15 of Advocate General Paolo Mengozzi, *supra* note 29, pp. 293

⁴⁹³ *Ibid.*, pp. 294

⁴⁹⁴ 2014 EU-Canada PNR Agreement, *supra* note 12, pp. 14(2)

⁴⁹⁵ *Ibid.*, pp. 14(1)

⁴⁹⁶ Opinion 1/15 of Advocate General Paolo Mengozzi, *op. cit.*, pp. 315, 320.

procedures to the EU.⁴⁹⁷ Thus, the Agreement implies to provide certain information to travelling public regarding its use and processing of PNR data through publication on its website.⁴⁹⁸ Moreover, it is foreseen in the 2012 EU-USA PNR Agreement for the Parties to work alongside with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.⁴⁹⁹

As regards access to PNR data and correction or rectification of PNR data, the 2012 EU-USA PNR Agreement maintains similar provisions as 2007 PNR Agreement. Thus, under the 2007 EU-USA PNR Agreement DHS made a policy decision to extend administrative Privacy Act protections to PNR data stored in their databases regardless of the nationality or country of residence of the data subject, including data that relates to European citizens.⁵⁰⁰ Consistent with U.S. law, DHS also maintained a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR which was not a case under 2004 EU-USA PNR Agreement.⁵⁰¹

Therefore, 2012 EU-USA PNR Agreement provides that “[...] any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS [...] may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS”⁵⁰². Thus, any refusal or restriction of access and any refusal or restriction of the correction or rectification shall be set forth in writing including the legal basis of such refusal or restriction and provided to the requesting individual on a timely basis and has to notify individual of the options available under US law to seek redress.⁵⁰³ However, 2012 EU-USA PNR Agreement provides that disclosure of information contained in PNR may be subject to reasonable legal

⁴⁹⁷ 2012 EU-USA PNR Agreement, *supra* note 11, pp. 10(2).

⁴⁹⁸ *Ibid.*, pp. 10(1).

DHS shall provide information to the travelling public regarding its use and processing of PNR through:

- (a) publications in the Federal Register;
- (b) publications on its website;
- (c) notices that may be incorporated by the carriers into contracts of carriage;
- (d) statutorily required reporting to Congress; and
- (e) other appropriate measures as may be developed.

⁴⁹⁹ *Ibid.*, pp. 11(3), 12(3).

⁵⁰⁰ 2007 EU-USA PNR Agreement, *supra* note 69, Title IV, US letter to EU.

⁵⁰¹ *Ibid.*, Title IV, US letter to EU.

⁵⁰² 2012 EU-USA PNR Agreement, *op. cit.*, pp. 11(1);

⁵⁰³ *Ibid.*, pp. 11(1), 11(2)

limitations which can be appointed under US, including limitations protecting privacy, national security and law enforcement sensitive information.⁵⁰⁴ ANNEX attached to the thesis particularly provides the procedure of the request to access PNR data by a data subject concerned. In particular, DHS was communicated by an individual concerned who has taken flight to USA in 2012 to receive PNR data relating to him. However, it appears from the response of US Citizenship and Immigration Service that in order to receive PNR data the request is deemed to constitute an agreement to pay any fees that may be chargeable up to twenty five (25) US dollars. According to the letter, fees may be charged for searching for records sought at the respective clerical, professional and/or managerial rates of four/seven/ ten twenty five (4, 5, 10.25) US dollars per quarter hour, and for duplication of copies at the rate of ten (10) US cent per copy. However, letter does not consist of the information whatever PNR data can be disclosed at all and how much the person concerned has to pay in order to receive information. Financial burden put on passengers may constitute interference to the right of access to data which has been collected concerning him. However, as it was notified by the letter, the request made by the person concerned constituted complex track, therefore, due to the increasing number of requests received by the office, the processing of the request encountered some delay.

Notwithstanding that, 2012 EU-USA PNR Agreement provides better safeguards than it was introduced under 2014 EU-Canada PNR Agreement, that is to say, DHS is obliged not to disclose PNR data to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by US law.⁵⁰⁵ Therefore, this approach seems to be compatible with Article 7, 8 and 52(1) of the Charter.

As regards administrative and judicial redress, the 2012 EU-USA PNR Agreement provides that “[...] any individual whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with US law”⁵⁰⁶. New to the 2012 PNR Agreement is the reference to explicitly detailed concept of judicial review when compared to 2007 EU-USA PNR Agreement. It is stated that, any individual is entitled to administratively challenge DHS decisions related to the use and processing of PNR.⁵⁰⁷ However, this provision does not entail any reference to the authority which

⁵⁰⁴ 2012 EU-USA PNR Agreement, supra note 11, pp. 11(1), 11(2)

⁵⁰⁵ Ibid, pp. 11(4).

⁵⁰⁶ Ibid., pp. 13(1).

⁵⁰⁷ 2012 EU-USA PNR Agreement, supra note 11, pp. 13(1).

is entitled to receive, investigate and respond to complaints lodged by an individual concerning their request for access, correction or notation of their PNR data which is explicitly required by Article 8(3) of the Charter, to be exact, complaints has to be investigated by an independent authority. Therefore, taking into account provisions on the oversight enshrined in the 2012 EU-USA PNR Agreement this authority appears to be the Department Privacy Officers, to be exact, DHS Chief Privacy Officer⁵⁰⁸ who have a proven “[...] record of autonomy; exercise effective powers of oversight, investigation, intervention, and review; and have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate”.

According to the Agreement, Department Privacy Officers have to ensure that complaints relating to non-compliance with this Agreement are received, investigated, responded to, and appropriately redressed.⁵⁰⁹ Thus, these complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence. Therefore, even though provision on administrative redress does not make reference to this authority required by 8(3) of the Charter, the oversight by independent public authority which is competent to examine complaints brought by individuals regardless of nationality, country of origin, or place of residence is provided in the 2012 EU-USA PNR Agreement. Therefore, it does not infringe the Article 7, 8 and 52(1) of the Charter.

Notwithstanding that, “[...] any individual is entitled to petition for judicial review in US federal court of any final agency action by DHS” providing relevant US laws and provisions⁵¹⁰. Even, DHS provides all individuals an administrative means⁵¹¹ to resolve travel-related inquiries including those related to the use of PNR providing a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat.⁵¹² Any such aggrieved individual is entitled to petition for judicial review in US federal court from any final agency action by DHS relating to such concerns.⁵¹³

⁵⁰⁸ Ibid., pp. 14(1).

⁵⁰⁹ Ibid., pp. 14(1).

⁵¹⁰ Ibid., pp. 14(3).

Any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

- (a) the Freedom of Information Act;
- (b) the Computer Fraud and Abuse Act;
- (c) the Electronic Communications Privacy Act; and
- (d) other applicable provisions of US law.

⁵¹¹ Ibid., pp. 14(4). currently the DHS Traveller Redress Inquiry Program (DHS TRIP)).

⁵¹² 2012 EU-USA PNR Agreement, *supra* note 11 pp. 14(4).

⁵¹³ Ibid., pp. 14(4). Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110,

As regards information to passengers, the 2012 EU-Australia PNR Agreement same as other Agreements implies Australia a duty to make available to the public information on the purpose of collection and use of PNR by the Australian Customs and Border Protection Service. In particular, this information has to be available on relevant government websites and include information on how to request access correction and redress.⁵¹⁴

The 2012 EU-Australia PNR Agreement maintains the same provisions as its predecessor regarding individuals' right to access as well as right to seek rectification of and require erasure of PNR data processed by Australian Customs and Border Protection Service regardless of their nationality or country of origin, place of residence or physical presence in Australia.⁵¹⁵ Any refusal or restriction of access, rectification or erasure of has to be set out in writing to the individual providing the factual or legal reasons on which the decision is based shall also be communicated to him or her.⁵¹⁶

What is relatively new that 2012 EU-Australia PNR Agreement further extends the right of access to the ability to request and to obtain documents held by the Australian Customs and Border Protection Service "[...] as to whether or not data relating to him or her have been transferred or made available and information on the recipients or categories of recipients to whom the data have been disclosed"⁵¹⁷. However, with due regard for the legitimate interest of the individual concerned disclosure of information may be "[...] subject to reasonable legal limitations applicable under Australian law to safeguard the prevention, detection, investigation, or prosecution of criminal offences and to protect public or national security".⁵¹⁸ Rather identical provision was introduced by 2014 EU-Canada and 2012 EU-USA PNR Agreement. Nonetheless, Australia as well as USA provides that competent authority to disclose PNR information, in this case, the Australian Customs and Border Protection Service, shall not disclose PNR data to the public, except to the individuals whose PNR data have been processed or their representatives.⁵¹⁹ This approach as identified under 2012 EU-USA PNR Agreement appears be compatible with 7, 8 and 52(1) of the Charter as

⁵¹⁴ Ibid., pp. 11(1,2)

⁵¹⁵ Ibid., pp. 12(1),13(1) see also 2012 EU-Australia PNR Agreement, supra note 11, pp. 7(1) and Annex, pp. 16-25.

⁵¹⁶ 2012 EU-Australia PNR Agreement, *ibid.*, pp. 12(3), 13(3).

⁵¹⁷ Ibid., pp. 12(1)

⁵¹⁸ Ibid., pp. 12(2)

⁵¹⁹ 2012 EU-Australia PNR Agreement, supra note 11, pp. 12(5).

implying obligation not to disclose data to anyone but directly related person or his/her representative.

In all of the abovementioned cases, individuals have to be informed of their right to lodge a complaint against the decision of the Australian Customs and Border Protection Service. This complaint has to be lodged to the Australian Information Commissioner who is entitled to formally advise persons concerned of the outcome of the investigation of the complaint.⁵²⁰ Therefore, the individual shall be further informed of the means available under Australian law for seeking administrative and judicial redress.⁵²¹

Furthermore, the 2012 EU-Australia PNR Agreement gives more clarity regarding individual's right to redress. By all means, any individual regardless of their nationality or country of origin, place of residence or physical presence in Australia is granted the right to effective administrative and judicial redress if any of his or her rights referred to in this Agreement have been violated as well as the right to apply for effective remedies, which may include compensation from Australia or to lodge a complaint to Australian Information Commissioner against the decision taken by Australian Customs and Border Protection Service to refuse or restrict access to PNR data⁵²². Moreover, in the same manner as under its predecessor and both 2012 EU-USA and 2014 EU-Canada PNR Agreements, 2012 EU-Australia PNR Agreement provision regarding effective administrative redress provides a right to individual concerned regardless of his or her nationality or country of residence to lodge a complaint to a public authority which has effective powers to hear this claims, to be exact, this public authority appears to be the Australian Information Commissioner.⁵²³ Even though, the 2012 EU- Australia PNR Agreement as regards administrative redress makes reference to a particular authority which has powers to undertake claims by individuals regardless of his or her nationality or country of residence both 2012 EU-USA and 2014 EU-Canada PNR Agreements require that public authority to be autonomous and impartial however this requirement is nowhere to be seen under 2012 EU-Australia PNR Agreement. Therefore, suffice to say, if this authority appears to be not fully independent from a political nature on the part of the authority to which it is responsible it cannot be regarded as an independent supervisory authority for

⁵²⁰ Ibid., , pp. 12(3-4).

⁵²¹ Ibid., pp. 12(4).

⁵²² Ibid., pp. 14,12.

⁵²³ Ibid., pp. 10(1,3), 12(3).

the purposes of Article 8(3) of the Charter. Therefore, the possibility that such a situation may arise, means that the contracting parties have not struck a fair balance between the objectives pursued by the Agreement therefore is incompatible with 7, 8 and 52(1) of the Charter.

After careful assessment on the guarantees for and rights of data subjects under 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements it has to be observed that all of the Agreements provide clear and precise information about their rights in particular about the right of access to his or her PNR data and the right to seek rectification and deletion of his or her PNR data in addition to the available redress effective mechanisms. Provisions as regards the right to access PNR data and the right to seek correction, rectification or deletion of PNR data and the right to seek effective administrative and judicial redress appears to be almost identical. All of the Agreements have the same provision which provides any individual regardless of his or her nationality or country of residence to enjoy all of the abovementioned rights. All of the Agreements must provide oversight by a public authority to receive, investigate and respond to complaints lodged by an individual concerning their request for access, correction or notation of their PNR data. This oversight is particularly required by the Article 8(3) of the Charter to ensure protection and security of the data collected PNR data. If independent supervisory authority would not be competent to examine requests of this kind or if this authority not fully enjoys independence from a political nature on the part of the authority to which it is responsible it cannot be regarded as an independent supervisory authority for the purposes of Article 8(3) of the Charter. The possibility that such a situation may arise, means that the contracting parties have not struck a fair balance between the objectives pursued by the Agreement therefore is incompatible with 7, 8 and 52(1) of the Charter. In the light of aforementioned the 2014 EU-Canada PNR Agreement fails to provide for any reference to this competent authority. This indicates that this public authority may be either incompetent or not fully independent to examine requests for access, correction or notation of their PNR data. Even though, the 2012 EU-Australia PNR Agreement as regards administrative redress makes reference to a particular authority which has powers to undertake claims by individuals regardless of his or her nationality or country of residence however this public authority has to be to be autonomous and impartial however this requirement is nowhere to be seen under 2012 EU-Australia PNR Agreement. Therefore, suffice to say, if this authority appears to be not fully independent from a political nature on the part of the authority to which it is responsible it cannot be regarded as an independent supervisory authority for the purposes of Article 8(3) of the Charter. Even though

provision on administrative redress does not make reference to independent public authority required by 8(3) of the Charter, the oversight by independent public authority which is competent to examine complaints brought by individuals regardless of nationality, country of origin, or place of residence is provided in the 2012 EU-USA PNR Agreement. Therefore, it does not infringe the Article 7, 8 and 52(1) of the Charter.

Additionally, it has to be observed that under 2014 EU-Canada PR Agreement as regards provision on a right to access PNR data in particular provision governing “any disclosure of information [...], regarding the legitimate interests of the individual concerned” provides neither the recipients of that information nor the use for which it may be requested. This particularly broad nature of the provision seems to go beyond what is strictly necessary to attain the public security objective pursued by the Agreement. Therefore, this provision is disproportional and incompatible with the Article 7, 8 and 52(1) of the Charter. Both, 2012 EU-USA and 2012 EU-Australia Agreements provide better safeguards in the light of this aspect. In particular, Australia as well as USA is obliged not disclose PNR data to the public, except to the individuals whose PNR data have been processed or their representatives. This approach seems to be proportional therefore compatible with Article 7, 8 and 52(1) of the Charter.

After assessing provisions on the use of PNR data, data elements to be collected, data retention periods, disclosure of data, the guarantees for and rights of data subjects introduced by 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements it has to be observed that in all cases PNR Agreements have attempted to preserve proportionality of public security and the fundamental right for protection of his private life and his own personal data. However, certain provisions happen to exceed what was strictly necessary to preserve public security objective therefore are incompatible with Articles 7 and 8 and Article 52(1) of the Charter. As it was mentioned in Section 2.1. international PNR Agreements concluded by EU with Canada, USA and Australia are valid only if they are consistent with EU primary law. However, in the light of aforementioned, it has to be observed that 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements are incompatible with the Charter, therefore invalid.

CONCLUSIONS AND PROPOSALS

The fight against serious transnational crime and terrorism is of the utmost importance to ensure public security, therefore PNR Agreements which are seeking to prevent, combat, repress, and eliminate these crimes genuinely satisfies public security objective. Nonetheless, 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements are incompatible with the fundamental rights enshrined in the Charter, i.e. respect for private and family life, guaranteed by Article 7, and the protection of personal data, guaranteed by Article 8, and therefore are illegal.

All PNR Agreements authorize process and transfer PNR data for purposes not properly related to the prevention of and combating terrorism. The 2012 EU-Australia PNR Agreement authorises the use of PNR data by Australia for the protection of the vital interests of any individual, the 2014 EU-Canada PNR Agreement additionally authorises competent authorities to use PNR data in order to comply with the subpoena, warrant or court order. In addition, the 2012 EU-USA PNR Agreement authorises competent authorities to use PNR data for border control purposes or other violations of law or indications thereof and by later undermining “criminal offences”. The use of PNR data should be implemented without further exceptions, i.e. EU-sourced PNR data should be used only for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime. All PNR Agreements should be accompanied by an exhaustive list of the offences coming within the definition of “serious transnational crime”.

As regards data elements to be collected, some of the categories under all the PNR Agreements are formulated in a very excessively, open manner, without being able to determine either the nature or the scope of the personal data, which these categories may contain. The categories of data in the Annexes to the Agreements should be drafted in a more concise and more precise manner, without any discretion being left to either the air carriers or the competent authorities as regards the actual scope of these categories to understand what data is to be regarded as having to be deleted by these authorities. The categories of data in the Annexes to the Agreements should be drafted in a manner to exclude any field which may apt to contain sensitive data which currently allows information about the health or ethnic origin or religious beliefs of the passenger concerned and and/or of those travelling with him to be disclosed. Further processing of sensitive data should be explicitly excluded.

As regards data retention periods, data retention periods should be clearly divided into two categories, which is not the case now: where the collected information relates to a person who is not the subject of an investigation and where the collected information relates to a person who is the subject of a further investigation. The Agreements should indicate objective reasons that could lead to increasing the PNR data retention period, which are missing in the current texts. The excessive period of data retention for 15 years provided by the 2012 EU-USA PNR Agreement cannot be justified as necessary, because the Agreement does not provide any objective reasons and does not substantiate the need for it. Agreements should be drafted in a manner to show that it is necessary to retain all the PNR data for a maximum period of retention, otherwise the data retention periods for different PNR data elements should be differentiated. At the end of data retention expiry period all the PNR data should be permanently deleted which is not the case under current 2012 EU-USA PNR Agreement.

All of the PNR Agreements as regards internal disclosure of PNR data should be accompanied by an exhaustive list of the government authorities entitled to receive PNR data which is currently a case under 2012 EU-Australia PNR Agreement. All of the PNR Agreements should prohibit external disclosure of PNR data if the receiving third country authority has not agreed not to further transfer PNR data. Only the 2012 EU-Australia PNR Agreement precludes such external disclosure of PNR data. If Australian competent authority is not satisfied, it may not disclose PNR data to the receiving third authority. This provision has never been introduced by the 2014 EU-Canada and 2012 EU-USA Agreements. All the PNR Agreements should introduce “ex ante” review of PNR data by the concerned competent authority of the Member State of the EU citizen or resident before that PNR data is transferred to a third country. A review of the disclosure of the data will not permit to counterbalance and incorrect assessment of the level of protection or to restore the confidentiality and privacy of the data when it has already been transferred and used by the recipient public authority. The best example can be seen in the case of the disclosure of data to a third country, where its successive use will be outside the competence and review of the competent authorities and courts.

As regards the guarantees for and rights of data subjects, PNR data should not be disclosed to the public, except to the individuals whose PNR data have been processed or their representatives. Both 2012 EU-USA and 2012 EU-Australia PNR Agreements adhere to this procedure. By the 2014 EU-

Canada PNR Agreement any disclosure of information or the use for which it may be requested shall be communicated to any natural or legal person, for instance a bank. To ensure protection of individuals with regard to the processing of personal data, all of the PNR Agreements should explicitly provide internal autonomous oversight, an independent public authority to receive, investigate and respond to the complaints lodged by an individual concerning their request for access, correction or notation of their PNR data. This authority should enjoy complete independence from a political nature on the part of the authority to which it is responsible and competence to examine requests of that type. If independent supervisory authority appears be not competent to examine requests of this kind or if this authority not fully enjoys independence from a political nature on the part of the authority to which it is responsible it could not be regarded as an independent supervisory authority explicitly required for the purposes of Article 8(3) of the Charter. Only 2012 EU-USA Agreement clearly provides this safeguard.

PNR Agreements themselves provide joint reviews for the purpose of revising implementation of the Agreements, both Parties policies and practices towards PNR data for the purpose of contributing effective operation and privacy protection of processing PNR. All the joint reviews undertaken by Parties as regards EU-USA PNR Agreements were concerning almost identical provisions to be improved. Even though it was acknowledged that the implementation of some commitments was technically and operationally challenging, the overall outcomes in all the Joint reviews resulted in conclusions that USA and Australia had implemented the Agreements in line with the conditions set out therein. This questions the effectiveness of the joint review procedure and its contribution to the operation and privacy protection of processing PNR. Consequently, non-compliance with undertaken obligations may have resulted in the suspension or termination of Agreements in the light of EU primary law. However, this was not the case. By identifying the incompliance of PNR agreements with the EU primary law the provisions of the agreements are perplexing to change.

BIBLIOGRAPHY

Agreements and Conventions

1. 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 O.J. (L 183) 84-85.
2. 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, OJL 298, 27.10.2006.
3. 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), OJL 204, 4.8.2007
4. Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012,
5. Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJL 82, 21.3.2006.
6. Proposal for a Council Decision on the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, COM(2013) 529final, Annex Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data.
7. Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, OJL 213, 8.8.2008, p. 49.
8. Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, L 186, 14/07/2012, p. 4, pp. 1

9. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.
10. European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5.

EU primary and secondary law

11. Consolidated version of the Treaty on the Functioning of the EU, OJ C 326, 26.10.2012, p. 47–390.
12. Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, 2006/253/EC, OJL 91, 29.3.2006, p. 49, Annex, Commitments by the Canada Border Service Agency in Relation to the Application of its PNR Program.
13. Charter of Fundamental Rights of the EU, 7 December 2000, OJ C 364.
14. Consolidated version of the Treaty on EU, OJ C 326, 26.10.2012, p. 13–390
15. Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the EU, of an Agreement between the EU and Australia on the processing and transfer of EU-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, OJL 213, 8.8.2008, p. 47.
16. Council Decision 2012/380/EU of 22 September 2011 on the signing, on behalf of the Union, of the Agreement between the EU and Australia on the processing and transfer of passenger name record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJEU L 186, 14.7.2012, p. 2.
17. Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24, 6.8.2004.
18. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

19. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89–131
20. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
21. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 24 October 1995.
22. European Parliament recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the EU and Australia on the processing and transfer of EU sourced passenger name record (PNR) data by air carriers to the Australian customs service (2008/2187(INI)), OJEU C 15E, 21.1.2010.
23. European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144.
24. European Parliament recommendation of 22 October 2008 to the Council concerning the conclusion of the Agreement between the EU and Australia on the processing and transfer of EU sourced passenger name record (PNR) data by air carriers to the Australian customs service (2008/2187(INI)), OJEU C 15E, 21.1.2010, p. 46.
25. European Parliament Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, and on the recommendations from the Commission to the Council to authorise the opening of negotiations between the EU and Australia, Canada and the United States, OJEU C 74E, 13.3.2012, p. 8.

26. Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, SEC(2011) 133 final.
27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

Foreign Legislative Acts

28. 49 USC 44939 note, Aviation and Transportation Security Act (ATSA), Public Law 107–71, November 19, 2001, SEC. 115. PASSENGER MANIFESTS
29. Canada Border Services Agency, Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data , Memorandum D1-16-3, Ottawa, May 31, 2016 ISSN 2369-2391, Superseded memorandum D1-16-3 dated January 14, 2010.

Opinions/Guidelines and Working Papers

30. Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, 00569/13/EN WP 203.
31. Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passenger's Data (13 06 2003), p. 7.
32. Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM (2010) 492 final, 21.9.2010.
33. 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 14 May 2004, Brussels, 12.12.2005, COM (2005) final.
34. Explanations relating to the Charter of Fundamental Rights of the European Union, document CONVENT 49 of 11.10.2000.

35. International Civil Aviation Organization “Guidelines on Passenger Name Record (PNR) data”, Approved by the Secretary General and published under his authority, First Edition — 2010.
36. Joint Review of the implementation of the Agreement between the EU and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security Accompanying the Report from the Commission to the European Parliament and to the Council on the joint review of the implementation of the Agreement between the EU and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, {COM(2013) 844 final}, Brussels, 27.11.2013, SEC(2013) 630 final.
37. Joint Review Report of the implementation of the Agreement between the EU and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service Accompanying the Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the EU and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service {COM(2014) 458 final}, Brussels, 10.7.2014, SWD(2014) 236 final.
38. Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (Vienna, 14 June 2011).
39. Opinion of the European Data Protection Supervisor on the proposal for a Council decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service OJ C 322, 5.11.2011.
40. Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines, WP 88, 11 February, Brussels.

41. Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Done in Brussels, 30 September 2013,

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-09-30_Canada_EN.pdf [last accessed 12-27-2016].

42. Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, Done in Brussels, 9 December 2011,

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-12-09_US_PNR_EN.pdf [last accessed 12-27-2016]

43. Opinion of the European Data Protection Supervisor on the proposal for a Council decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (2011/C 322/01).

44. Opinion of the Article 29 Working Party, (2012)15841 - 06/01/2012, pp. 8. < http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf> [last accessed 12-27-2016].

45. Report on the joint review of the implementation of the Agreement between the EU 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, Brussels, 7.4.2010.

46. The Article 29 Working Party Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries (WP 178), adopted on 12 November 2010 and the EDPS Opinion of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of

Passenger Name Records to the United States Department of Homeland Security, OJ C 35/03, 09.02.2012, p.16.

47. The Commissioner for Human, “Rights Protecting the right to privacy in the fight against terrorism”, CommDH/IssuePaper(2008)3, Strasbourg, 4 December 2008 pp. 4
48. The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary.
49. WCO/IATA/ICAO “Guidelines on Advance Passenger Information (API)”, 2010.

Articles and Books

50. Blasi Casagran, C., “Global Data Protection in the Field of Law Enforcement– An EU Perspective”, Routledge Taylor & Francis Group, London and New York, 2017.
51. Guild, E. and Brouwer, E., “The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US”, CEPS Policy Brief No. 109, CEPS, Brussels, 26 July 2006.
52. Gutwith, S., Leenes, R., De Hert, P., Pouillet, Y., editors, “European Data Protection: In Good Health?” Springer Dordrecht Heidelberg London New York, 2012, Franziska Boehm, Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems
53. F. de Londras, Doody, J. “The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism”, Routledge, Taylor&Francis Group, 2015.
54. Hobbing, P., Tracing Terrorists: The EU-Canada Agreement in PNR Matters CEPS Special Report/September 2008.
55. Hornung G., Boehm, F., “Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security “ Passau/Luxembourg, 14 March 2012.

56. Hustinx, P., "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation".
57. Kaunert, C., Leonard, S. and Pawlak, P., Contemporary Security Studies, European Homeland Security– A European Strategy in the Making?, MacKenzie, A. "The external dimension of European homeland security", p. 95 -111, First published 2012 by Routledge 2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN.
58. Kozłowski, R., "Border and Transportation Security in the Transatlantic Relationship", in A. Dalgaard-Nielsen and D.S. Hamilton (eds), Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism, London/New York, 2006, pp. 89–105.
59. Louks, D., "(Fly) Anywhere but here: approaching US-US dialogue concerning PNR in the era of Lisbon", Int'l & Comp. L. Rev. 479 2013.
60. Nino, M., "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 62 2010.
61. Rossi Dal Pozzo, F., "EU Legal Framework for Safeguarding Air Passenger Rights", Springer International Publishing Switzerland 2015.

Case-law of the Court of Justice of the European Union

62. Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU, Opinion 1/15, 2015/C 138/32.
63. Joined Cases C-317/04 and C-318/04, European Parliament. Council of the European Union, PNR, [2006] ECR I-04721.
64. Joined Cases C-293/12 and C-594/12 [2014], ECLI:EU:C:2014:238.
65. Case-366/10 - Air Transport Association of America and Others [2011] ECR 13755.
66. Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063.

67. Case -407/08 P Knauf Gips v Commission [2010] ECR I-6375.
68. Case T-187/11 Mohamed Trabelsi and Others v Council of the EU [2013], ECLI:EU:T:2013:273.
69. Case-473/12 IPI EU:C:2013:715.
70. Case C-343/09 Afton Chemical EU:C:2010:419.
71. Cases C-581/10 and C-629/10 Nelson and Others EU:C:2012:657.
72. Case C-283/11 Sky Österreich EU:C:2013:28.
73. Case C-101/12 Schaible EU:C:2013:661.

Opinions of the Advocate General of the Court of Justice of the European Union

74. Opinion 1/15 of Advocate General Paolo Mengozzi, ECLI:EU:C:2016:656.
75. Opinion of Advocate General Kokott delivered on 6 October 2011 Case C-366/10 Air Transport Association of America and Others, ECLI:EU:C:2011:637.

Cases law of the European Court of Human Rights

76. Klass v Germany, *Application no. 15473/89*, 22 September 1993
77. Khelili v Switzerland, *Application no. 16188/07*, 1 October 2011
78. Malone v United Kingdom, *Application no. 8691/79*, 2 August 1984.
79. Leander v Sweden, *Application no. 9248/81*, 26 March 1987.
80. Gaskin v United Kingdom, *Application no. 10454/83*, 07 July 1989.
81. Niemietz v Germany, *Application no. 13710/88*, 16 December 1992.
82. Halford v United Kingdom, *Application 20605/92*, 25 June 1997.
83. Amann v Switzerland, *App No 27798/95*, 16 February 2000.
84. Rotaru v Romania, *Application no. 28341/95*, 4 May 2000.

85. S. and Marper v. the United Kingdom, Application no. 30562/04 and 30566/04, 4 December 2008.
86. Segerstedt-Wiberg and Others v Sweden, Application no 62332/00, 6 June 2006.
87. M.M. v UK, Application no. 24029/07, 13 November 2012.
88. Weber and Saravia v. Germany Application no. 54934/00) [2006] Admissibility Decision, 29 June 2006.

Internet sources:

89. Article 29 Data Protection Working Party, and to the letter of 6 January 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf [last accessed 12-06-2016]
90. Council of the EU, Signature of the EU-Canada agreement on Passenger Name Records (PNR), Brussels, 25 June 2014, 10940/14, PRESSE 339.< [http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-\(pnr\)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-a](http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-a)> [last accessed 12-27-2016]
91. Court of Justice of the EU, “The Court of Justice declares the Data Retention Directive to be invalid”, PRESS RELEASE No 54/14, Luxembourg, 8 April 2014, <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> [last accessed 12-27-2016]
92. Council of the EU, Signature of the EU-Canada agreement on Passenger Name Records (PNR), Brussels, 25 June 2014, 10940/14, PRESSE 339 [http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-\(pnr\)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-ab](http://webcache.googleusercontent.com/search?q=cache:3rd2rPqt124J:www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/+&cd=1&hl=lt&ct=clnk&gl=us&client=firefox-b-ab) [last accessed 12-27-2016]

93. European Parliament, “EU Passenger Name Record (PNR) directive: an overview”, Justice and home affairs, 01-06-2016, <[http://www.europarl.europa.eu/news/lt/news-room/20150123BKG12902/eu-passenger-name-record-\(pnr\)-directive-an-overview](http://www.europarl.europa.eu/news/lt/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview) > [last accessed 11-20-2016].
94. European Digital Rights (EDRi) by Diego Naranjo, FAQ: Passenger Name Records (PNR), 09 Dec 2015, <https://edri.org/faq-pnr/>, [last accessed 12-5-2016]
95. European Digital Rights (EDRi) <https://edri.org/theme/privacy/> [last accessed 12-06-2012]
96. European Parliament, “Sources and scope of EU law”, Fact Sheets on the EU, Udo Bux, 10/2016, p. 1 http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf [last accessed 12-27-2016]
97. European Commission official webpage “Protection of personal data”, <http://ec.europa.eu/justice/data-protection/> [last accessed 12-08-2016]
98. Estelle Massé,”Advocate General opinion on EU Canada PNR agreement: it won’t fly”, 8 September 2016, <https://www.accessnow.org/advocate-general-opinion-eu-canada-pnr-agreement-wont-fly/> [last accessed 11-24-2016]
99. Dov Waxman, “Living with terror, not Living in Terror: The Impact of Chronic Terrorism on Israeli Society”, Perspectives on terrorism, Vol 5, No 5-6 (2011), ISSN 2334-3745, <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/living-with-terror/html> [last accessed 12-25-2016].
100. Joint Media release with Minister for Home Affairs, The Hon Bob Debus MP 1 July 2008 on Australia and the EU Sign Passenger Name Record (PNR) Agreement, <http://foreignminister.gov.au/releases/2008/fa-s080701.html> [last accessed 10/20/2016].
101. International Air Transportation Association (IATA), Passenger Data Exchange: The Basics,<http://www.iata.org/iata/passenger-data-toolkit/presentation.htm> [accessed 11.17.2016].

102. Mark Feldman “The Travel Adviser: No show, no fly”, 09/26/2015, <
<http://www.jpost.com/Not-Just-News/The-Travel-Adviser-No-show-no-fly-419193>> [last
accessed 12/10/16]
103. Milon Gupta, Privacy and Data Protection in the EU in Eurescom message, issue
3/2011 [http://www.eurescom.eu/fileadmin/documents/message/EURESCOM_message_03-
2011.pdf](http://www.eurescom.eu/fileadmin/documents/message/EURESCOM_message_03-2011.pdf) [last accessed 11.24.2016].

ANNOTATION

Constantly increasing wave of terrorism attacks and transnational crime rate called for new technological developments in the society to be used to fight this cross-border phenomenon. PNR data is currently viewed as one of the key tool in the fight against terrorist offences and serious transnational crimes. After 9/11 attacks in USA countries such as USA, Canada and Australia started to require air carriers arriving at their territory to submit PNR data. Therefore, to comply with requirements and to increase international cooperation in the area of fight against terrorism and serious transnational crimes the EU has concluded Agreements on the processing and transfer of EU-sourced PNR data with USA, Canada and Australia. Although data and privacy protection was often seen as an obstacle to effective anti-terrorist measures, it was crucial to the maintenance of fundamental democratic values.

While assessing two strong opposing forces, the desire to uphold fair balance between public security and the fundamental right for everyone of protection of his privacy and his own personal data it was found that all PNR Agreements exceeds what is strictly necessary to attain the public security objective. Therefore are incompatible with Article 7, 8 and 52(1) of the Charter. Thus, bilateral PNR Agreement concluded by EU with Canada, USA and Australia are inconsistent with EU the primary law, therefore invalid.

Substantial words/phrases: bilateral PNR Agreements, EU primary law, privacy and data protection, compatability with the Charter, fight against terrorism and serious transnational crimes.

ANOTACIJA

Nuolat augantis terorizmo išpuolių ir tarptautinio nusikalstamumo lygis paskatino naujus technologinius išradimus visuomenėje panaudoti kovojant su šiuo tarpvalstybiniu reiškiniu. Keleivių duomenų įrašo (PNR) duomenys šiuo metu vertinami kaip vienas iš pagrindinių įrankių kovoje su teroristiniais nusikaltimais ir sunkiais tarptautiniais nusikaltimais. Po 9/11 išpuolių Amerikoje tokios šalys kaip JAV, Kanada ir Australija pradėjo reikalauti, kad oro vežėjai, atvykstantys į jų teritorijas pateiktų PNR duomenis. Todėl, kad būtų laikomasi šalių nustatytų reikalavimų, ir stiprinti tarptautinį bendradarbiavimą kovojant su terorizmu ir sunkiais tarptautiniais nusikaltimais ES sudarė

susitarimus dėl Europos Sąjungos surinktų PNR duomenų naudojimo ir perdavimo su JAV, Kanada ir Australija. Nors duomenų ir privatumo apsauga dažnai buvo vertinama kaip kliūtis įgyvendinant priemonės veiksmingai kovai su terorizmu, tai buvo labai svarbu siekiant užtikrinti pagrindinių demokratinių vertybių priežiūrą.

Vertinant dvi stiprias priešingas jėgas, norą palaikyti pusiausvyrą tarp visuomenės saugumo ir pagrindinės teisės visiems apsaugoti savo privatumą ir savo asmeninius duomenis, buvo nustatyta, kad visi PNR susitarimai viršija tai, kas būtina užtikrinti visuomenės saugumą. Todėl yra nesuderinama su Chartijos 7, 8 ir 52(1) straipsniais. Taigi, dvišaliai PNR susitarimai kuriuos ES sudarė su Kanada, JAV ir Australija yra nesuderinamas su ES pirminė teise, todėl yra negaliojantys. **Reikšminiai žodžiai / frazės:** dvišaliai PNR susitarimai, ES pirminė teisė, privatumas ir duomenų apsauga, suderinamumas su Chartija, kova su terorizmu ir sunkiais tarptautiniais nusikaltimais.

SUMMARY

The master thesis strive to provide assesment of the legality of EU bilateral PNR Agreements concluded with non-EU countries, in particular, Canada, USA and Australia.

In order to reduce tremendously growing wave of terrorism attacks and transnational crime rate, new technological developments in the society is called to fight this cross-border phenomenon. Among such tools are API and PNR data. API data is limited in scope, different from and should not be confused with PNR data. API data does not facilitate the detection of hitherto ‘unknown’ criminals and are mainly used as identity verification and border management tool. Whilst, PNR data can be used to identify a person, but it might be used for customs, law enforcement purposes, security and more importantly risk-based assessment of persons about whom one may not have collected any information, and is typically more valuable in the identification of suspicious trends, relationships and travel patterns. Therefore, PNR data is currently viewed as one of the key tool in the fight against terrorist offences and serious transnational crimes.

Although the use of PNR data has become harmonized at the EU level by adopting EU PNR Directive on the 27 of April 2016, the use of PNR data is not currently harmonized at the international level. Meanwhile, after 9/11 attacks in the USA a number of non-EU countries started to require air carriers arriving at their territory to submit PNR data. USA, Canada and Australia are among those countries. Therefore, EU was confronted with the urgent choice of either facing heavy fines/ loss of the landing rights in the territories of the countries or potentially infringing EU data protection laws. Therefore, to comply with requirements and to increase international cooperation in the area of fight against terrorism and serious transnational crimes, the EU concluded bilateral Agreements on the processing and transfers of EU-sourced PNR data with USA, Canada and Australia.

Bilateral PNR Agreement concluded by EU with Canada, USA and Australia have to be consistent with the primary law of the EU. In particular, PNR Agreements must be consistent with the provisions of the Charter relating to respect for private and family life, guaranteed by Article 7, and

the protection of personal data, guaranteed by Article 8. In the light of 52(1) of the Charter limitations to enjoy high level of privacy and personal data protection may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or are in need to protect the rights and freedoms of others. Furthermore, the balance between strong conflicting forces, the desire to maintain public security and the equally fundamental right for everyone to be able to enjoy a high level of protection of his private life and his own personal data must be preserved.

In that regard, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security therefore processing, using, storing and transferring of EU-sourced PNR data by competent US, Canadian and Australian authorities seeking to prevent, combat, repress, and eliminate terrorism and terrorist-related offences, as well as other serious transnational crime genuinely satisfied public security objective.

However, after assessing mostly criticized provisions on the use of PNR data, data elements to be collected, data retention periods, disclosure of data, the guarantees for and rights of data subjects introduced by 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements it has to be observed that in all cases PNR Agreements have attempted to preserve proportionality of public security and the fundamental right for protection of his private life and his own personal data. However, certain provisions happen to exceeded what was strictly necessary to preserve public security objective therefore are incompatible with Articles 7 and 8 and Article 52(1) of the Charter. Therefore, 2014 EU-Canada, 2012 EU-USA and 2012 EU-Australia PNR Agreements are incompatible with EU primary law and invalid.

SANTRAUKA

Baigiamajame magistro darbe siekiama įvertinti ES sudarytų dvišalių Keleivių duomenų įrašo (PNR) susitarimų su trečiosiomis šalimis, konkrečiai Kanada, JAV ir Australija, teisėtumą.

Siekiant sumažinti nepaliojamai augantį terorizmo išpuolių ir tarptautinio nusikalstamumo lygis, nauji technologiniai išradimai visuomenėje yra pasitelkiami kovai su šiuo tarpvalstybiniu reiškiniu. Tarp tokių priemonių yra Išankstinės informacija apie keleivius (API) ir Keleivių duomenų įrašo

(PNR) duomenys. API duomenų apimtis yra ribota, todėl skiriasi nuo ir neturėtų būti painiojamas su PNR duomenimis. API duomenimis nėra palengvinamas iki šiol "nežinomų" nusikaltėlių aptikimas, todėl jie dažiausiai naudojami kaip tapatybės tikrinimui ir valstybės sienų priežiūrai. Nors, PNR duomenys gali būti naudojami siekiant nustatyti asmens tapatybę, tačiau jie turėtų būti naudojami muitinės, teisėsaugos ar saugumą tikslais, ypač siekinat įvertinti rizikingų asmenų, apie kuriuos nėra jokios informacijos, taip pat siekiant įvertinti įtartinas tendencijas, santykius ir kelionių kryptis. Todėl, PNR duomenys šiuo metu vertinamai kaip vienas iš pagrindinių įrankių kovoje su teroristiniais nusikaltimais ir sunkiais tarptautiniais nusikaltimais.

Nors PNR duomenų naudojimas tapo suderintas ES lygmeniu priimant ES PNR direktyvą 2016 m balandžio 27 dieną, PNR duomenų naudojimas šiuo metu nėra suderintas tarptautiniu lygiu. Tuo tarpu, po 9/11 išpuolių JAV keletas trečiųjų šalių iš pradėjo reikalauti, kad oro vežėjai, atvykstantys į jų teritorijas pateiktų PNR duomenis. JAV, Kanada ir Australija buvo tarp tų šalių. Todėl ES privalėjo imtis skubių priemonių kitaip jai grėsė didelės baudos ir/ar nusileidimo teisės tų šalių teritorijose praradimas arba potencialus ES duomenų apsaugos teisės aktų pažeidimas. Siekiant laikytis reikalavimų, ir stiprinti tarptautinį bendradarbiavimą kovojant su terorizmu ir sunkiais tarptautiniais nusikaltimais srityje, ES sudarė dvišalius susitarimus dėl ES surinktų PNR duomenų naudojimo ir perdavimo su JAV, Kanada ir Australija.

Dvišaliai PNR susitarimai sudaryti ES su Kanada, JAV ir Australija turi būti suderinami su pirmine ES teise ES. Konkrečiai susitarimai privalo atitikti Chartijos nuostatas, susijusias su teise į privatų ir šeimos gyvenimą, garantuojamą 7 straipsnyje, ir asmens duomenų apsaugą, garantuojamą 8 straipsnyje. Atsižvelgiant į Chartijos 52(1) straipsnį aukšto lygio privatumo ir asmeninių duomenų apsaugos teisė gali būti apribojama tik tada, jei apribojimai yra būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba yra reikalingi apsaugoti kitų asmenų teises ir laisves. Todėl norint išsaugoti viešąjį saugumą ir vienodai pamatines teises kiekvienam mėgautis aukšto lygio asmens privatumo ir asmeninių duomenų apsauga, stiprių priešingų jėgų balansas turi būti išsaugotas.

Šiuo atžvilgiu reikia konstatuoti, kad kova su sunkiais nusikaltimais, ypač su organizuotu nusikalstamumu ir terorizmu, iš tiesų yra labai svarbu, siekiant užtikrinti visuomenės saugumą. Todėl ES surinktų PNR duomenų apdorojimas, naudojimas, saugojimas ir perduodavimas kompetentingoms JAV, Kanados ir Australijos valdžios institucijoms, siekiančios užkirsti kelią,

kovoti, nuslopinti ir panaikinti terorizmą ir su terorizmu susijusius nusikaltimus taip pat kitus sunkius tarpvalstybinių nusikaltimus tikrai atitinka visuomenės saugumo tikslą.

Tačiau įvertinus labiausiai kritikuotas 2014 ES-Kanados, 2012 ES-JAV 2012 ES-Australijos PNR susitarimų nuostatas dėl PNR duomenų naudojimo, surenkamų duomenų elementų, duomenų saugojimo laikotarpių, duomenų dalijimosi/perdavimo, duomenų subjektų teisių ir garantijų, turi būti pasakyta, kad visais atvejais PNR susitarimai bandė išsaugoti proporcingumą tarp visuomenės saugumo ir pagrindinių privataus gyvenimo ir asmens duomenų teisių apsaugos. Tačiau kai kurios nuostatos akivaizdžiai viršijo tai, kas buvo būtina išsaugoti visuomenės saugumą, todėl yra nesuderinamos su 7, 8 and 52 (1) Chartijos straipsniais. Todėl 2014 ES- Kanados, 2012 ES-JAV ir 2012 ES ir Australijos PNR susitarimai yra nesuderinami su ES pirmine teise ir negalioja.

U.S. Department of Homeland Security
National Records Center
P.O. Box 648010
Lee's Summit, MO 64064-8010



U.S. Citizenship
and Immigration
Services

November 15, 2016

UNP2016003798

Dear

We received your request for information relating to Egle Beinoryte on November 15, 2016.

Your request is being handled under the provisions of the Freedom of Information Act (5 U.S.C. § 552). It has been assigned the following control number: UNP2016003798. Please cite this number in all future correspondence about your request.

We respond to requests on a first-in, first-out basis and on a multi-track system. Your request has been placed in the complex track (Track 2). You may wish to narrow your request to a specific document in order to be eligible for the faster track. To do so, please send a written request, identifying the specific document sought, to the address above. We will notify you if your request is placed in the simple track.

Consistent with 6 C.F.R. § 5.5(a) of the Department of Homeland Security (DHS) FOIA regulations, USCIS processes FOIA requests according to their order of receipt. Although USCIS' goal is to respond within 20 business days of receipt of your request, FOIA does permit a 10-day extension of this time period in certain circumstances. Due to the increasing number of FOIA requests received by this office, we may encounter some delay in processing your request. Additionally, due to the scope and nature of your request, USCIS will need to locate, compile, and review responsive records from multiple offices, both at headquarters and in the field. USCIS may also need to consult with another agency or other component of the Department of Homeland Security that have a substantial interest in the responsive information. Due to these unusual circumstances, USCIS will invoke a 10-day extension for your request pursuant to 5 U.S.C. § 552(a)(6)(B). Please contact our office if you would like to limit the scope of your request or to agree on a different timetable for the processing of your request. We will make every effort to comply with your request in a timely manner.

In accordance with Department of Homeland Security Regulations (6 C.F.R. § 5.3(c)), your request is deemed to constitute an agreement to pay any fees that may be chargeable up to \$25.00. Fees may be charged for searching for records sought at the respective clerical, professional, and/or managerial rates of \$4.00/\$7.00/\$10.25 per quarter hour, and for duplication of copies at the rate of \$.10 per copy. The first 100 copies and two hours of search time are not charged, and the remaining combined charges for search and duplication must exceed \$14.00 before we will charge you any fees. Most requests do not require any fees; however, if fees in excess of \$25.00 are required, we will notify you beforehand.

www.uscis.gov

UNP2016003798

Page 2

This office will be providing your records on a Compact Disc (CD) for use on your personal computer. The CD is readable on all computers through the use of Adobe Acrobat software. A version of Adobe Acrobat will be included on the CD. Your records can be viewed on your computer screen and can be printed onto paper. Only records 15 pages or more are eligible for CD printing. To request your responsive records on paper, please include your control number and write to the above address Attention: FOIA/PA Officer, or fax them to (816) 350-5785.

In order to continue processing your request, we ask that you provide the following: **See attached.** Please note your control number with any correspondence you send. Please provide this information within 30 days of the date of this letter; otherwise your request will be administratively closed as a failure to comply.

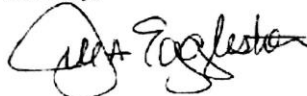
USCIS no longer collects Social Security Numbers in connection with FOIA or PA requests. When forwarding to us any documents related to your request, please ensure any Social Security Numbers on the documents are blanked out or removed.

The National Records Center (NRC) has the responsibility to ensure that personally identifiable information (PII) pertaining to U.S. Citizenship and Immigration Services (USCIS) clients is protected. In our efforts to safeguard this information, we may request that additional information be provided to facilitate and correctly identify records responsive to your request. Though submission of this information is voluntary, without this information, your request may be delayed while additional steps are taken to ensure the correct responsive records are located and processed. Further, if we are unable to positively identify the subject of the record we may be unable to provide records responsive to your FOIA request.

You may check the status of your FOIA request online, at www.uscis.gov. Click on "Check Status of Request" button located on the middle of the webpage. If you have any questions concerning your pending FOIA/PA request, or to check the status of a pending application or petition, please call The National Customer Service Center at 1-800-375-5283. Please be aware that the National Records Center no longer accepts FOIA/PA related questions directly by phone.

All FOIA/PA related requests, including address changes, must be submitted in writing and be signed by the requester. Please include the control number listed above on all correspondence with this office. Requests may be mailed to the FOIA/PA Officer at the PO Box listed at the top of the letterhead, or sent by fax to (816) 350-5785. You may also submit FOIA/PA related requests to our e-mail address at uscis.foia@uscis.dhs.gov.

Sincerely,



Jill A. Eggleston
Director, FOIA Operations

CONFIRMATION OF INDEPENDENCE OF THE WRITTEN WORK

Form approved by Resolution No. 1SN-10 of the Senate
of Mykolas Romeris University of 20 November 2012

CONFIRMATION OF INDEPENDENCE OF THE WRITTEN WORK

20 - -
Vilnius

I, Mykolas Romeris University (hereinafter referred to as the University),

(Faculty / Institute, study programme)

Student _____,
(Name, surname)

hereby confirm that this academic paper / Bachelor's / Master's final thesis

“ _____
_____ ”:

1. Has been accomplished independently by me and in good faith;
2. Has never been submitted and defended in any other educational institution in Lithuania or abroad;
3. Is written in accordance with principles of academic writing and being familiar with methodological guidelines for academic papers.

I am aware of the fact that in case of breaching the principle of fair competition – plagiarism – a student can be expelled from the University for the gross breach of academic discipline.

(Signature)

(Name, surname)