**EALA PRIZE 2015**

# Passenger Data Protection in the European Union: The Long and Winding Road

July 2015

**Ridha Aditya Nugraha**

[Abstract: This paper explains passenger data protection issues in the European Union (EU) which is under threat at the moment. The protection level under the current legal framework in this region have proven to be insufficient to secure EU citizens' privacy through the processing of passengers' personal data. Invalidity of the Data Retention Directive in force and sentiments towards the EU-USA Passengers Name Record Agreement are the portraits of the darkest days for EU airline passengers. Finally, there is an urgent need for a new Data Protection Regulation to ensure no fundamental rights are infringed.]

## Table of Contest

## A. Introduction

Owning privacy is one of the most important things in life. Living in the 21st century, which is associated with the digital era, the term 'privacy' has evolved into personal data that is 'scattered' on the internet. The European Union (EU), as the leading regional policy maker has taken a role in guarding its citizens' privacy by establishing legal framework which are Directive (EC) No. 46 Year 1995[1] and Regulation (EC) No. 45 Year 2001[2]. However, no specific legal framework has been made in relation with airline passengers' personal data protection. A question that arises is whether these legal framework are still up-to-date with the current technology innovations. Otherwise there will be a loophole within the positive laws which means personal data protection is in danger.

As of today, information technology (or known as IT) plays a vital role within the fast growing aviation business. One of its significant contributions is the current booking system through the Internet which is user-friendly and accessible 24/7. This innovation looks simple but, beyond that, it establishes a great responsibility for airlines (in this paper 'airlines' shall mean EU airlines) to process and secure their passengers' data in good order according to the legal framework mentioned above. In order to secure the data, passenger data protection issues should not be separated from data retention framework within the EU. This paper discusses these issues and the current and future legal challenges, including the EU-USA Passenger Name Records Agreement of 2012 where the fate of EU citizens' data is at stake and the new draft on EU Data Protection Regulation.

[1] Directive (EC) No. 46 of Year 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data as amended with Regulation (EC) No. 1882 of Year 2003 adapting to Council Decision 1999/468/EC the Provisions Relating to Committees Which Assist the Commission in the Exercise of its Implementing Powers Laid Down in Instruments Subject to the Procedure Referred to in Article 251 of the EC Treaty.

[2] Regulation (EC) No. 45 of Year 2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data.

B. What is in a Name? 'Privacy'

Living in a digital era where many things fade away, privacy could be considered as one of them. With numerous definitions of privacy, Gellert and Gutwirth defined this term as:

> "*How to cope with information stemming from social interaction in a way that certain areas of one's personal life are hidden from unwanted views*."[3]

Privacy is considered broader than mere personal data in terms of profiling[4].[5] Personal data itself is defined as any information relating to an identified or identifiable natural person.[6] But it must also be noticed that the misuse of personal data could have a significant effect on someone's privacy.[7] To simplify, privacy is a matter of opacity and personal data under data protection is related to transparency.[8]

The technological evolution of digitalization could threaten key aspects of fundamental citizens' rights, such as the rights to privacy, data protection, non-discrimination, and also the core value of the European societies, democracy.[9] Hiding behind national security interests, the state as the main actor, consistently wishes to have access and control of all data including personal data. For example in Germany, national

---

[3] Raphael Gellert and Serge Gutwirth, "Beyond Accountability, the Return to Privacy?" in Daniel Guagnin *et.al.* (eds.), Managing Privacy Through Accountability, (Houndmills: Palgrave Macmillan, 2012), page 261-284 as stated in Francesca Bosco *et.al.*, "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities" in Serge Gutwirth, Ronald Leens, and Paul de Hert (eds.), Reforming European Data Protection Law, (Dordrecht: Springer, 2015), page 16.

[4] Profiling is not defined in Article 2 under the "Defintion" section in Regulation (EC) No. 45 of Year 2001, thus there is no special explanation about it. However, it is defined within the new Data Protection Regulation draft as any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

[5] *Supra* note 3, page 16.

[6] The Netherlands, Article 1 of *Wet Bescherming Persoonsgegevens* of 2000.

[7] Francesca Bosco *et.al.*, "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities" in Serge Gutwirth, Ronald Leens, and Paul de Hert (eds.), Reforming European Data Protection Law, (Dordrecht: Springer, 2015), page 16.

[8] *Supra* note 3, page 16.

[9] *Supra* note 7, page 12.

authorities host large numbers of distinct databases for various purposes which potentially infringe on both EU and non-EU citizens' privacy.[10] The last Charlie Hebdo incident has given a fresh wind to the authorities who are seeking more comprehensive access to personal data for the prevention of another radical attack. In order to achieve a 'balance' in the EU, data protection together with data retention legal framework are set up to facilitate the free flow of information by safeguarding all matters related to personal data.[11]

## C. Data Protection in the European Union

Data protection in the EU is regulated under Directive (EC) No. 46 Year 1995 and Regulation (EC) No. 45 Year 2001 (Data Protection Legal Framework) which both have been in existence for more than a decade. These legal framework are based on Article 8 of the European Convention on Human Rights which grants the EU citizens the right to protection of their private life.[12] With the speed of current technological development, it could be said that this legislation is not able to keep up, a fact which maybe considered the major weak point. Passengers' personal data within the EU is also subject to these legal framework due the absence of *lex specialis* for airline passengers. As one of the legal framework comes under a 'directive' as mentioned above, this means each member state has flexibility to accommodate it within their national laws. For example, in the Netherlands, it became the *Wet Bescherming Persoonsgegevens* of 2000[13] which obviously has differences with data protection laws in Germany or Spain.

The European Data Protection Supervisor (EDPS) was established in 2001 to ensure that all EU institutions and bodies, including airline companies, respect people's right to privacy when processing their personal data and also to advise them on all aspects of personal data

[10] *Supra* note 7, page 14.

[11] *Supra* note 7, page 16.

[12] Christopher Rees, "Who Owns Our Data?", *Computer Law and Security Review*, Volume 30 (2014), page 76.

[13] The Netherlands, *Wet Bescherming Persoonsgegevens* of 2000.

processing.[14] The term 'processing' is defined as several activities; collecting information, recording and storing, retrieving it for consultation, sending it or making it available to other people, and also blocking, erasing, or destroying data.[15] There is a delegation of supervision authority by the EDPS to each member state, which is an impact of decentralitation with the aim of providing a more effective, efficient, and broader supervision.

Speaking of personal data processing, there are several data categories to which data processors are normally prohibited from accessing. The access to these categories is defined according to the current legal framework and these categories come under very strict rules if access is ever allowed. These categories are i.) religion or philosophical belief; ii.) race or ethnic origin, with the exception of identifying the country of birth; iii.) political opinions; iv.) health life; v.) sexual life; vi.) trade union membership; and vii.) criminal behaviour.[16] As the data subject, every airline passenger has the right to obtain information from the airline company or the relevant authority within a certain time whether personal data relating to them is being processed. In the event that the processed data is factually inacurate, incomplete, or irrelevant to the purpose of data processing, the data subject has the right to request from the airline that their personal data be deleted or blocked.[17] The EDPS, or its national extension within the member states, is the institution where a data subject can bring any dispute related to personal data. Failure to settle it at the EDPS level may end up at the Court of Justice of the European Union (CJEU) as the last guardian of personal data within this regional initiative.

The EU has already shown its strong commitment protecting its citizens' personal data and privacy through the Huber Case[18] and the Bavarian Lager Case[19] which are explained briefly below.

---

[14] http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm as accessed in 25 May 2015.

[15] http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm as accessed in 25 May 2015. See also Article 2(b) of the Regulation (EC) No. 45 of Year 2001.

[16] Article 10 of the Regulation (EC) No. 45 of Year 2001.

[17] See Section 5, Article 13 to 19 of the Regulation (EC) No. 45 of Year 2001.

[18] Case No. C-524/06 Huber *versus* Federal Republic of Germany, judgement of 16 December 2008.

i. The Huber Case[20]

In Germany a centralised register is held which contains personal data and details relating to foreign nationals, both for EU and non-EU citizens, who reside in Germany for more than three months. This data is used to different ends such as for statistical purposes and for crime fighting, while at the same time there is no comparable database for German nationals. Mr. Huber, as an Austrian national who resides in Germany, brought this issue before the administrative court where the latter referred it to the CJEU concerning the compatability of the processing of personal data within the German centralised register with the prohibition on any discrimination on grounds of nationality as provided in the European Community (EC) Treaty and Directive (EC) No. 45 Year 1995.

The Court pointed out that Germany's nationals cannot be differentiated from the nationals of other member states. Since the German register does not contain the personal data of German nationals, the systematic processing of personal data relating only to nationals of other member states for the purposes of fighting crime is considered discrimination on grounds of nationality which is prohibited by Article 12 of the EC Treaty and Article 18 of the Treaty on the Functioning of the European Union (TFEU).

ii. The Bavarian Lager Case[21]

Bavarian Lager is a company established in 1992 for the importation of bottled German beer into the United Kingdom which encountered difficulties due to the fact that since most publicans were tied down by exclusive purchasing contracts to obtain supplies from certain British breweries and legislation in the UK at the time *de facto* favoured these national contracts. The

[19] Case No. C-28/08 P Commission *versus* Bavarian Lager, judgement of 29 June 2010.

[20] See the summary at http://ec.europa.eu/dgs/legal_service/arrets/06c524_en.pdf as accessed in 24 May 2015.

[21] See the summary at http://ec.europa.eu/dgs/legal_service/arrets/08c028_en.pdf as accessed in 25 May 2015.

company submitted this case which led into an amendment of UK law. Subsequently the company requested the European Commission (Commission) for a copy of the minutes of a meeting which also had been attended by the British authorities. The Commission granted this request by forwarding the minutes of the meeting with five names which had been blacked out according to Article 8(b) of Regulation (EC) No. 45 Year 2001. The company was not satisfied with this and referred it to the General Court (a UK Court) which passed the decision on to the CJEU, where the latter concluded that the Commission was right in checking whether the attendees at the meeting agreed to the disclosure of their names. This case specifies the limits of the right of access to documents under the rules for the protection of personal data.

These court decisions show that EU policies as intepreted by the CJEU are in favour of the protection of personal data and privacy, superseeding any state's interest with regards to security concerns.

## D. The Darkest Days for the EU Airline Passengers

Nowadays passenger data protection in the EU is under threat. Digitalization of passenger transactions does not only produce data but also provides information which can be used to extract knowledge about individuals.[22] Once stored via the internet, for example through the purchase of an airline ticket, data become easily exchangable worldwide.[23] Despite privacy issues, airlines and travel agents, in a highly competitive world, have welcomed this digitized era with their main objective being the processing of data automatically in an easier and cheaper way[24], thus leaving the burden of personal data protection solely to the Commission. Unfortunately this situation is worsened because the various EU institutions involved in data protection do not have a common agenda nor do they operate in harmony due to political

[22] *Supra* note 7, page 9.

[23] *Supra* note 7, page 9.

[24] *Supra* note 7, page 8.

constraints, institutional ambitions, and power-struggles.[25] A complex situation of passenger data protection practices in the EU will be described futher below.

### D.1. Invalidity of the Present Data Retention Directive

Questions about where and how personal data is stored causes much controversy. Due to this fact, data protection should not be separated from data retention. Data retention comes under Directive (EC) No. 24 Year 2006[26] (Data Retention Directive) which is relatively new compared to the existing two Data Protection Legal Framework. Knowing that the data retention directive was created almost a decade ago, the same question for data protection has arisen: is the directive still up-to-date and relevant with the current digital technology world?

According to this directive, the period of data retention shall be between six months and not more than two years.[27] This means that no uniformity has been established because the period varies according to each member state's national laws. Passenger data shall be subject to appropriate technical and organizational measures to protect the data against unlawful storage, processing, access or disclosure and also to ensure that they can be accessed by the authorised personnel only.[28] An obligation to destroy the data at the end of the period of retention exists within the Data Protection Directive under supervision of the public authority within each member state,[29] although in the end we cannot know whether it is already completely destroyed.

---

[25] Paul de Hert and Vagelis Papakonstantinou, "The EU Institutions' Battle Over Data Processing vs Individual Rights" in Florian Trauner and Ariadna Ripoll Servent (eds.), Policy Change in the Area of Freedom, Security and Justice, (New York: Routledge, 2015), page 185.

[26] Directive (EC) No. 24 of Year 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Network and Amending Directive 2002/58/EC.

[27] Article 6 of the Data Retention Directive.

[28] Article 7 of the Data Retention Directive.

[29] Articles 7 and 9 of the Data Retention Directive.

Last year, the CJEU made a decision which was a shocking result for the EU where the CJEU declared the Data Retention Directive to be invalid and that it infringed upon the fundamental rights to privacy and to the protection of personal data.[30] The court observed that the data taken may provide very precise information on the private lives of the persons whose data is retained, such as permanent or temporary places of residence, daily or other movements, and activities carried out.[31] Purchasing airline tickets via the internet is definitely relevant with this. Futhermore the CJEU took the view that,

> *"…by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particulary serious manner with the fundamental rights to respect for private life and to the protection of personal data."*[32]

The Data Retention Directive has generated a feeling among EU citizens that their private lives are the subject of constant surveillance due the lack of safeguards provided in the directive to ensure effective protection of the data against any risk of abuse.[33] The other key weak spot is that this directive does not require the data be retained within the EU, therefore no absolute control could be carried out effectively on the basis of EU law.[34]

At the moment passenger data protection within the EU is in danger because no revision towards the current Data Retention Directive has been made. A short conclusion could be withdrawn that the objective of Data Retention Directive to keep passenger data secured is merely an utopia.

---

[30] CJEU Press Release No. 54/14 on Judgement in Joined Cases C-293/12 and C-594/12 regarding Digital Rights Ireland and Seitlinger and Others on 8 April 2014.

[31] *Ibid*.

[32] *Ibid*.

[33] *Ibid*.

[34] *Ibid*.

D.2. Are the EU Airlines Really Protecting Their Passengers' Data?

Obviously airlines, as one of the parties who benefit from technology in this digital era,[35] have an obligation to protect their passengers' data under the current Data Protection Legal Framework. This obligation consists of how an airline company establishes an internal policy towards its employees' access to passengers' data, how the marketing division should 'behave' while promoting special offers, and how the right information and consent requests have been delivered to the passenger regarding his/her personal data.

Establishing and maintaining the internal policy with regards to the level of access permitted with passenger data updated within an airline company is an important task which has yet to be completed. This effort, which comes under the Data Protection Legal Framework, will determine who is the controller[36] and who is the processor[37], especially the latter among the airline's employees working with passenger data processing. The purpose of identifying the controller and processor is to clearly establish employees' tasks and responsibilities in order to avoid data mismanagement, thus setting up the airline as a fellow custodian alongside the CJEU guarding data protection. One key questions which must be answered is how to ensure that all EU airlines have correctly interpreted and implemented the Data Protection Legal Framework and the Data Retention Directive while considering that the fact remains that there is no uniformity within the member states due to the nature of a directive. This will lead us to

[35] Richard Kemp, "Legal Aspects of Managing Big Data", *Computer Law and Security Review*, Volume 30 (2014), page 485.

[36] According to Article 2 (d) of the Data Protection Regulation No. 45 Year 2001, controller shall mean the Community institution of body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act.

[37] According to Article 2 (e) of the Data Protection Regulation No. 45 Year 2001, processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

question whether the absence of any specific case law[38] within air transportation, between any party versus airlines (and its subsidiaries or partners), regarding passenger data protection until today means that the EU airlines are going about things the right way or that there exists a loophole in EDPS supervision.

How to store the passengers' personal data is one the most important issues. In regards to efficiency of data processing, the airline customarily works with another company specialising in data storage service or sub-contracts this work out. If the airline does not maintain sufficient control, there is a need for strenghtening privacy within the service or sub-contract agreement.[39] The solution looks relatively straightforward, but are EU airlines able to translate this into one or two short sentences within the agreement as they have today with its data storage provider?

Limiting the employees access within the home server sounds very simple, but it has very important consequences. A finance staff should not have unrestricted access to IT department documents, which could process any passengers' personal data, through a simple click a computer. A restricted account which has variation of levels towards each employee based on his/her position is needed. Also followed with an immediate update on the employees' access if he/she is transferred to another department. This situation shows how important of having an internal framework to protect the passengers' personal data, furthermore securing the airline company from any charge or suit on grounds of not performing the Data Protection Legal Framework.

In a highly competitive world, airlines' marketing divisions are promoting to get passengers' attention aggressively. Supported by

[38] See http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm as accessed in 30 May 2015.

[39] Georgia Skouma and Laura Léonard, "On-line Behavioural Tracking: What May Change After the Legal Reform on Personal Data Protection" in Daniel Guagnin *et.al.* (eds.), Managing Privacy Through Accountability, (Houndmills: Palgrave Macmillan, 2012), page 261-284 as stated in *supra* note 7, page 58.

technology known as 'cookies'[40], airlines are able to process passenger behaviour to offer them the right promotion. Cookies as the backbone of their marketing drives, the marketing division can analyze each person using algorithms to adduce some conclusions about the interests and buying habits of the tracked persons.[41] This 'cookies' method is already subject to the Data Protection Legal Framework insofar as they process information that identifies or may potentially identify a natural person.[42] Nowadays it often happens if you ever searched or booked a specific route through a website, for example Paris-Copenhagen, that many offers for this route will appear when you open other websites. This marketing practice seems to become common now and airlines must ask for permission, in the clearest way, to use cookies for their passengers' internet launcher when accessing the website. An ambiguity appears towards the word "ask for permission" whether just "informing", through terms and conditions section which usually appears almost unseen or very small at the bottom of the website, is already considered sufficient.

Airlines must be extremely careful when using the processed personal data by avoiding sensitive words for its promotions that could reveal relationship status, sexual orientation, and philosophical beliefs.[43] For example there must not be a special promotion only for Catholics to go to Vatican during Christmas or a special discount only for LGBT couples, either implictly or explicitly, by ticking a special clickbox during ticket purchase.

Group ticket is another interesting issue where it means each passenger with their code could take a look into the other passengers' personal data within the group. Even though they know each other, still, legally speaking it means a breach on Data Protection Legal Framework. Thus a prevention measure must be

[40] Cookies is defined as piece of text stored by a user's web browser and transmitted as part of an HTTP request. See Claude Castelluccia and Arvind Narayanan, "Privacy Considerations of Online Behavioural Tracking", European Network and Information Security Agency Report on 19 October 2012, page 6.

[41] *Supra* note 39, page 36.

[42] *Supra* note 39, page 36.

[43] *Supra* note 39, page 36.

done, either within the airline or travel agent booking system for giving access.

However, both the passengers and even the airlines could not know and secure themselves completely from hackers or third parties' illegal activities even though an adequate level of protection has been established within the website. But still in order to protect the passengers, it is the airline's obligation to notice a breach of data storage.

### D.3. Lessons from the EU-USA Passengers Name Record Agreements[44]

In the wake of the tragedy of 9/11, Western societies accepted some sacrifice of individual rights under the name of 'security' and since then the rationale of policy makers in these Western societies has tended towards being more security-oriented.[45] After the tragedy, US authorities started asking international airlines for access to passenger data, which also had to increase in accuracy and quantity.[46] Numerous EU airlines faced with a dilemma because the request seemed to contradict with their data protection obligations concerning passengers' personal data and also due to costs.[47] This situation lead to chaos, for example in Belgium, where the Belgian Data Protection Authority verified that two airlines did not inform the passengers that their data

[44] Passenger Name Records shall mean the record created by air carriers or their authorized agents for each journey booked by or on behalf of any passenger and contained in carriers' reservation system, departure control systems, or equivalent systems providing similar functionality. It includes information such as name, dates of travel and travel itinerary, ticket information, address and phone numbers, means of payment used, credit card number, travel agent, seat number and baggage information. See Article 2 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 of 19 April 2012. See also Council of the European Union Press Release No. 9186/12 on 26 April 2012.

[45] *Supra* note 25, page 180.

[46] *Supra* note 25, page 189.

[47] *Supra* note 25, page 189. See also Ioannis Ntovas, "Air Passenger Data Transfer to the USA: the Decision of the ECJ and Latest Developments", *International Journal of Law and Technology*, Volume 16 No. 1 (2007), page 77.

would be transferred to US authorities.[48] One of the airlines did inform their passengers, but according to the Belgian authority, their means of communication of this fact was not explicit enough, as the information was integrated into the general condition terms that were available upon request only or via the internet.[49]

This situation represents one of the major tests facing the EU with regards to protecting its citizens' data through the European Community (now the European Union) and United States of America Passengers Name Record Agreement (EU-USA PNR Agreement).[50] Following to this obligation, the European Court of Justice (ECJ) annuled the EU-USA PNR Agreement in 2006,[51] before a replacement agreement was reached a few months later.[52] The Treaty of Lisbon[53], created six years after the 2001 tragedy, marks a major milestone in data protection since the first data protection acts appeared in Europe around four decades ago.[54] This treaty empowers actors that favour a stronger emphasis on the individual's right to data protection and made significant contributions to the recent EU PNR Agreements with Australia, Canada, and especially the United States.[55] Under this legal framework, the EDPS issued its critical opinion on the proposal of the latest EU-USA PNR Agreements in 2011 that: i.) the 15-year retention period is excessive and data should be deleted

---

[48] Maria Verónica Pérez Asinari and Yves Poullet, "Airline Passengers' Data: Adoption of an Adequacy Decision by the European Commission. How Will the Story End?", *Computer Law and Security Report*, Volume 20 No. 5 (2004), page 373.

[49] *Ibid.*

[50] The EU-USA PNR Agreement was made in 2004, 2006, 2007, and lastly 2012.

[51] 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, attached to the Council decision of 17 May 2004 (2004/496/EC), OJ L 183 of 20 May 2004, as known as "The First EU-USA PNR Agreement".

[52] Ioannis Ntovas, "Air Passenger Data Transfer to the USA: the Decision of the ECJ and Latest Developments", *International Journal of Law and Technology*, Volume 16 No. 1 (2007), page 75.

[53] Article 16 of the Treaty No. C 306/01 Year 2007 amending the Treaty on European Union and the Treaty Establishing the European Community.

[54] *Supra* note 25, page 180.

[55] *Supra* note 25, page 180-185.

immediately after its analysis or after a maximum six months; ii.) the list of data to be transferred should be narrowed and exclude sensitive data; and iii.) the US Department of Homeland Security should not transfer the data to other US authorities or third countries unless they guarantee an equivalent level of protection.[56] No wonder if the EDPS reacted this way since EU airline passengers' privacy is at stake, especially since non-US citizens do not benefit from the US Privacy Act of 1974[57].

As a result of the pressure, the main aspects of the EU-USA PNR Agreement of 2012, which is the latest and enforced, are a legally binding commitment form the US Department of Homeland Security to inform the Member States and EU authorities of any relevant intelligence from the analysis of these PNR data; and a limited usage of PNR data for a period of ten years for transnational crime and fifteen years for terrorism where the personally identifiable information of PNR data will be masked out after six months and will be moved to a dormant database with additional controls.[58] At least there is a limitation and masking measure, but still, should it be that long?

Some articles of the EU-USA PNR Agreement of 2012 which shows the weakness within the EU passengers' data protection could be pointed out as described below.

*Article 6(4)*

"*Sensitive data shall be permanently deleted not later than 30 (thirty) days...*"

[56] EDPS Press Release No. EDPS/12/11 on 13 December 2011.

[57] The United States of America, an Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes on 31 December 1974.

[58] Article 8 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 of 19 April 2012. See also Council of the European Union Press Release No. 9186/12 on 26 April 2012.

Even though personal data, such as race, religion, and sexual orientation, could not be exempted from being processed, at least there is a guarantee this data shall be permanently deleted within a certain period. This provision could be considered as a win-win solution between the fortress EU and the US that always want to know the who, what, when, why, and how of passengers to the country.

> *Article 5(2)(b)*
>
> "*PNR shall be held in a secure physical environment and protected with physical intrusions controls.*"

Still in connection with the previous article, this provision shows how the US will do its best to reassure the protection of the EU passengers' personal data to melt the fortress EU. However, it is interesting to see the next article as mentioned below.

> *Article 17(1)*
>
> "*The authority may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement…*"

This article tends contradict and destroy all of the safeguards that have been made by allowing PNR transfers to a third country. It seems those first two provisions above are just lip service, because PNR transfers to any third country means a potency for the EU losing its control towards its citizens' privacy. The absence of an effective control is more or less the same as having no protection towards EU passengers' personal data.

Furthermore the EU-USA PNR Agreements from time to time has shown the implementation of the jurisfaction and jurisaction theory within the real world. Bin Cheng's definitions of jurisfaction and jurisaction are as follows:

*Jurisfaction*

*"the normative element of State jurisdiction which entitles a State to make laws or take decision, including judicial decision, with legally binding effect within its own territory or world-wide extraterritorially."*[59]

*Jurisaction*

*"the concrete element of State jurisdiction which enables a Stage physically to carry out the functions of a State by setting up machinery to make laws and take decision, or by actually taking steps to implement and to enforce its laws and decisions."*[60]

An important battle over data protection is being fought between the EU and the US at the moment concerning whether the EU will be able to secure its jurisfaction on Data Protection Legal Framework across the Atlantic. The world is looking carefully at this battle over the fate of EU citizens' personal data. Another significant task for the European Commission is ensuring that its citizens and airlines to not become victims. As long as there are no supranational legal framework on Passengers Name Records in force, for example the Chicago Convention of 1944, 'small' states' or regional initiatives' legal framework outside its border tend only to achieve the jurisaction label.

Taking a look at this situation, the International Civil Aviation Organization (ICAO) should have establish a global standard with a high level of passenger data protection which applies to all citizens of member states.[61] It should come under hard law, not under ICAO's guidelines which are not binding thus do not solve

[59] Bin Cheng, "International Responsibility and Liability of States for National Activities in Outer Space Especially by Non-Governmental Entities" in Ronald St. John Macdonald (ed.), Essays in Honour of Wang Tieya, (Dordrecht: Martinus Nijhoff Publishers, 1994), page 146.

[60] *Ibid*.

[61] Arnulf S. Gubitz, "The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?", *New England Law Review*, Volume 39 (2005), page 472.

the problem.[62] However, without EU and American support, it seems unlikely that the ICAO's initiative on passenger data protection will work.[63]

## E. Urgency for a New Data Protection Regulation: Light after Darkness for EU and non-EU Passengers?

With the growth of technologies, new forms of tracking individuals have been invented.[64] Amongst those, online tracking systems which monitor users' behaviour, habits, and personality has proved its added-value primarily to marketing and advertising companies but also to other industries which deal with customer relationship management tools.[65] The implementation of this innovation could help an airline to create better services, but it may not be done at the expense of the consumer's privacy.[66] At the time that the Data Protection Legal Framework and Data Retention Directive were enacted, the EU legislator could not predict the overwhelming scale of Internet usage, especially online tracking tools in the form of (internet) cookies that we are all subject to nowadays.[67] In recent years, the emergence of social media, cloud computing, and smart phones which automatically collect personal data have added pressure to update the current legal framework.[68] These are two of the main reasons why a new Data Protection Regulation is needed where the current definitions will be redefined.[69]

Having seen the importance of personal data protection, especially today, a strong and uniform legal framework is needed to get the job done. Looking at the nature of hard law within the EU, the new legal framework must be a regulation and not a directive due to the binding

---

[62] Olga Mironenko Enerstvedt, "Russian PNR System: Data Protection Issues and Global Prospects", *Computer Law and Security Review*, Volume 30 (2014), page 29.

[63] *Supra* note 61, page 472.

[64] *Supra* note 39, page 35.

[65] *Supra* note 39, page 35.

[66] Tomi Mikkonen, "Perceptions of Controllers on EU Data Protection Reform: A Finnish Perspective", *Computer Law and Security Law Review*, Volume 30 (2014), page 190.

[67] *Supra* note 39, page 36.

[68] *Supra* note 66, page 190.

[69] *Supra* note 39, page 36.

power of a regulation, as opposed to a directive, which does not have such power. Currently the EU needs to show a strong hand in terms of regulating passenger data protection to win back its citizens' trust which has been affected by the EU-USA PNR Agreements issues.

The invalidity of the current Data Retention Directive must be seen as a chance for promoting more harmonisation between passenger data protection and how the data is stored. Now is the perfect time to integrate data retention provisions within the new draft of data protection regulation, or at least if they are still separated, then a clear and up-to-date relationship between them must be established. EU citizens and airlines must not become the next victims again. Stakeholders, such as EU citizens and aviation related associations, must take action by applying pressure to the Commission for establishing a more pro-data protection legislation which is supported by the readiness of EU institutions. It is time for EU aviation public foundations to speak louder for a special provision regarding airline passenger data considering the new Data Protection Regulation is not yet enacted. In the end, no matter how strong the new Data Protection Legal Framework is, it relies upon international cooperation to achieve its objectives.[70]

## F. Concluding Remarks and the Way Forward

Even though data protection is well guarded via its comprehensive legal framework in the EU, airline passenger data protection is at its lowest ebb because of many loopholes within the current Data Protection Legal Framework and Data Retention Directive. This situation has affected EU citizens as their privacy is under threat due to the European Commission's failure to keep up-to-date with technology development. The darkest days for airline passengers in the EU has come with the invalidity of the Data Retention Directive which has not been replaced with a current one, thus leaving data storage in chaos, and also leaves a significant question mark as to whether EU airlines are protecting their passengers' data in the right way. Passenger data protection in this region is being cornered by the existing EU-USA PNR Agreement, and this trend will continue in future if no strong stance has been taken by the European Commission.

[70] *Supra* note 25, page 192.

There is an urgent need to keep EU airline passengers' personal data protection back at the highest possible level by revising the current Data Protection Legal Framework and Data Retention Directive. Airlines must be really aware of their obligations towards its passengers' personal data. It is time for aviation stakeholder to pressure EU legislators, for the sake not only for passengers but also the airlines. Thus, efforts to force the EU to enact a new Data Protection Regulation should not be considered as merely a castle in the air.

## Bibliography

### Regional Legislative Acts

European Union. *Directive (EC) on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Directive No. 46 Year 1995.

European Union. *Directive (EC) on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Network and Amending Directive 2002/58/EC*. Directive No. 24 Year 2006.

European Union. *Regulation (EC) adapting to Council Decision 1999/468/EC the Provisions Relating to Committees Which Assist the Commission in the Exercise of its Implementing Powers Laid Down in Instruments Subject to the Procedure Referred to in Article 251 of the EC Treaty.* Regulation No. 1882 Year 2003.

European Union. *Regulation (EC) on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data*. Regulation No. 45 Year 2001.

European Union. *Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community*. Treaty No. C 306/01 Year 2007.

European Union. *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 of 17 May 2004*. The Passenger Name Record Agreement of 2004.

European Union. *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 of 19 April 2012*. The Passenger Name Record Agreement of 2012.

**National Laws**

The Netherlands. *Wet Bescherming Persoonsgegevens*. The Dutch Act of 2000.

The United States of America. *An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes.* The US Privacy Act of 1974.

**Cases**

*European Commission v The Bavarian Lager Co. Ltd*.. Case No. C-28/08 (European Court of Justice, judgement of 29 June 2010).

*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung*. Joined Case No. C-293/12 and C-594/12 (European Court of Justice, judgement of 8 April 2014).

*Heinz Huber v Bundesrepublik Germany*. Case No. C-524/06 (European Court of Justice, judgement of 16 December 2008).

**Books**

Guagnin, Daniel; *et.al.* (eds.). Managing Privacy Through Accountability. Houndmills: Palgrave Macmillan, 2012.

Gutwirth, Serge; Leenes, Ronald; and de Hert, Paul (eds.). Reforming European Data Protection Law. Dordrecht: Springer, 2015.

Macdonald, Ronald St. John (ed.). Essays in Honour of Wang Tieya. Dordrecht: Martinus Nijhoff Publishers, 1994.

Trauner, Florian and Servent, Ariadna Ripoll (eds.). Policy Change in the Area of Freedom, Security and Justice. New York: Routledge, 2015.

**Articles**

Asinari, Maria Verónica Pérez and Poullet, Yves. "Airline Passengers' Data: Adoption of an Adequacy Decision by the European Commission. How Will the Story End?". *Computer Law and Security Report Volume 20 No. 5* (2004).

Enerstvedt, Olga Mironenko. "Russian PNR System: Data Protection Issues and Global Prospects". *Computer Law and Security Review Volume 30* (2014).

Gubitz, Arnulf S.. "The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?". *New England Law Review Volume 39* (2005).

Kemp, Richard. "Legal Aspects of Managing Big Data". *Computer Law and Security Review Volume 30* (2014).

Mikkonen, Tomi. "Perceptions of Controllers on EU Data Protection Reform: A Finnish Perspective". *Computer Law and Security Law Review*, *Volume 30* (2014).

Ntovas, Ioannis. "Air Passenger Data Transfer to the USA: the Decision of the ECJ and Latest Developments". *International Journal of Law and Technology Volume 16 No. 1* (2007).

Rees, Christopher. "Who Owns Our Data?". *Computer Law and Security Review Volume 30* (2014).

**Websites**

http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm

http://ec.europa.eu/dgs/legal_service/arrets/06c524_en.pdf

http://ec.europa.eu/dgs/legal_service/arrets/08c028_en.pdf

http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm

**Miscellaneous**

Castelluccia, Claude and Narayanan, Arvind. "Privacy Considerations of Online Behavioural Tracking". European Network and Information Security Agency Report on 19 October 2012.

Court of Justice of the European Union. Press Release No. 54/14 on Judgement in Joined Cases C-293/12 and C-594/12 regarding Digital Rights Ireland and Seitlinger and Others on 8 April 2014.

Council of the European Union. Press Release No. 9186/12 on the new EU-US Agreement on Passenger Name Records (PNR) on 26 April 2012.

European Data Protection Supervisor. Press Release No. EDPS/12/11 on 13 December 2011.