Anggriawan, Rizaldy., Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. "Passenger Name Record Data Protection under EU and US Agreement: Security over Privacy?" *Hasanuddin Law Review* 8 no. 2 (2022): 95-1110. DOI: 10.20956/halrev.v8i2.2844

HasanuddinLawReview

Volume 8 Issue 2, August 2022
P-ISSN: 2442-9880, E-ISSN: 2442-9899

Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?

Rizaldy Anggriawan[1], Andi Agus Salim[2], Yordan Gunawan[3], Mohammad Hazyar Arumbinang[4]

[1] *Department of Financial and Economic Law, Asia University, Taiwan. E-mail: 108136043@live.asia.edu.tw*
[2] *Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia. E-mail: andi.agus@umy.ac.id*
[3] *Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia. E-mail: yordangunawan@umy.ac.id*
[4] *School of Law, University of Melbourne, Australia. E-mail: marumbinang@student.unimelb.edu.au*

Abstract: Privacy should become a key component in the IT system. It is not something to be considered at last but from the very early stages. Almost no nation has a greater sense of personal data security which could be equivalent to the European level. Since 9/11, the United States has declared to utilize PNR as a method for combating terrorism by associating PNR data with criminal records. Nevertheless, in fact, the majority of data found in the PNR is immense and most of this data is of a confidential nature. The paper used doctrinal legal research methodology utilizing the case and comparative law approach. It elaborates particular cases in relation to data protection issues. It also explores the differences between EU and US law which hinder the idea of data protection in particular on PNR. The study revealed that security is one of the most critical issues which hinder the agreement between the EU and the US on PNR data protection. As the EU promotes the highest standard to the data protection referring to the European community history and GDPR provisions, while the US places national security as a main priority beyond the privacy issues.

Keywords: Passenger Name Record; Data Protection; Security Cooperation; Aviation Security; Terrorism

1. Introduction

Personal data is an increasingly important issue in the last two decades, mainly due to the rapid progress made in the IT field.[1] In fact, in just two decades IT has progressed rapidly in storing data and information. Previous generations grew and experienced a rapid transition from floppy disks that could store several megabytes of information to years of use of CDs that allowed them to load gigabytes of data. Even now servers provided by cloud services are capable of storing terabytes and petabytes of data.[2] On the other hand, along with advances in the field of data storage, there have also been developments in internet technology. Today people no longer need to store thousands

[1] Soumitra Dutta, Thierry Geiger, and Bruno Lanvin. "The Global Information Technology Report 2015." In World Economic Forum, vol. 1, no. 1, pp. P80-85. 2015.

[2] Changqing Ji, Yu Li, Wenming Qiu, Uchechukwu Awada, and Keqiu Li. "Big Data Processing in Cloud Computing Environments." In *2012 12th international symposium on pervasive systems, algorithms and networks*, pp. 17-23. IEEE, 2012.

of sheets of paper on large shelves. Everything is loaded and stored on the web and easily accessed from anywhere and quickly and exchanged without geographic restrictions.[3]

Nevertheless, behind the sophistication and development of the technology, there is a massive and significant impact on a person's privacy rights.[4] In recent years there has been an explosion of phenomena on social networking platforms where every single day a large amount of the user's personal data is uploaded.[5] It is then feared that this could eliminate the boundaries of one's traditional privacy. The security of a large amount of personal data floating around the network is considered to be an issue and a big concern for its users.

Social networks and search engines derive most of their revenue from selling their users' personal data.[6] As for companies that have to deal electronically with the management of personal data stored on servers, they often do not guarantee an adequate level of protection for the data collected. It has been proven on more than one occasion that they did not fulfill their responsibility for the data. Every year there are many breaches in the company's IT systems where they reveal the data entered by the users. Even tech giants like Sony proved to be unreliable custodians when hackers broke into Japanese multinational servers in 2011, stealing the personal data of nearly 77 million people, including names, addresses, emails, and in some cases, including Credit Card Information.[7] In that case, Sony waited 7 days before notifying interested parties. This is devastating considering that there are data such as credit card numbers at stake. Had data protection laws been implemented globally, the Japanese company would have been penalized for failing to notify data subjects in a timely manner. But this is not the case at this time. Indeed, only a few countries have an acceptable level of security for a privacy policy.

Therefore, it is important of achieving joint laws that provide the security of one's personal data is guaranteed. This can be achieved by requiring a personal data manager to provide a high level of data protection. On the other hand, it is necessary to have a protocol that allows to immediately notify people in the event of a violation in the system, so that the affected users can immediately take the necessary actions to minimize losses.

It is unfortunate that there is currently no law on the protection of personal data that is applied internationally. Part of the difficulty in reaching an agreement arises from the fact that this is a morally controversial area where the right to expression has been seen and is still confronted with the national security and right to privacy. So far, Europe has risen to fight for the protection of personal data and the EU has approved regulations that

---

[3] Ronald Martinez, Karon A. Weber, Samantha Tripodi, Winton Davies, Chris Kalaboukis, and Oliver Raskin. "System and Method of Storing Data and Context of Client Application on the Web." *U.S. Patent 8,046,437*, issued October 25, 2011.

[4] Abraham L. Newman, "What the “Right to be Forgotten” Means for Privacy in a Digital Age." *Science* 347, no. 6221 (2015): 507-508.

[5] Seref Sagiroglu and Duygu Sinanc. "Big Data: A review." In *2013 international conference on collaboration technologies and systems (CTS)*, pp. 42-47. IEEE, 2013.

[6] Kalev Leetaru, ”What Does It Mean for Social Media Platforms to "Sell" Our Data*?,*” Accessed January 13, 2021, https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=240141022d6c.

[7] McKay Cunningham. "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law." *Geo. Wash. Int'l L. Rev*. 44 (2012): 643.

would eventually standardize laws on personal data protection among its member countries. The EU is the only international organization that may currently be able to initiate a process that could lead to the creation of an international agreement protecting the protection of personal data.

Despite the fact that Olsen's[8] and Lowe's[9] work acknowledged that there has been debate in the EU over the collecting and sharing of PNR data particularly caused by the issue of terrorism and mostly due to a lack of safeguards and protection of personal data. However, the reason for the earlier impediment to agreement legislation is unclear. To address the issue, a comparative analysis of the approaches taken by the two countries is required. Therefore, in this study, the paper investigated the latest legal developments regarding the protection of personal data within the EU and its relationship to some of the most important issues surrounding it. Furthermore, this research explores the path and approach that legislators have taken and also evaluates it differently from other countries, particularly the US. It will also elaborate the agreement on Passenger Name Record (PNR) data between the EU and the US. The issue of privacy and security will then be discussed further in the paper.

2. Method

This research is discussed and analyzed using doctrinal legal research methodology. Doctrinal legal research methodology elaborates legal issues based on previous legal doctrines or opinions that are relevant to the object of research being discussed. The doctrinal legal research method can be interpreted as a method of research on statutory rules both from the point of view of the hierarchy of statutory regulations (vertical), and the harmonious relationship of legislation (horizontal). Doctrinal law research methods use a normative juridical approach. The study also used a case and comparative approach, namely by studying the application of legal norms and rules in practice between the EU and the US. The case approach is carried out by examining cases related to the discussed object of research. The study analyzes the court decisions which legally binding and valid. The use of this case approach is based on the concept of *ratio decidendi*, which is legal reasons used by judges to arrive at their decisions. In cases that have been decided, these matters are then studied to obtain an overview of legal norms and rules in their application.

3. The EU and US Legal Framework on Data Protection

3.1. The Strasbourg Convention No. 108

A significant step forward was taken at the Council of Europe in 1981. The work which led to the opening and signing of the Strasbourg Convention No 108 on the protection of individuals with regard to automated processing of personal data (hereinafter 'Convention 108'), a legally binding international treaty on the protection of personal

[8] Henrik Palmer Olsen, and Cornelius Wiesener, "Beyond data protection concerns–the European passenger's name record system." *Law, Innovation and Technology* 13, no. 2 (2021): 398-421.

[9] David Lowe, "The European Union's passenger name record data directive 2016/681: Is it fit for purpose?" *International Criminal Law Review* 17, no. 1 (2017): 78-106.

data, was completed in that year.[10] In fact, the preamble points out the need to extend the protection of everyone's fundamental rights and freedoms, and in particular the right to respect for private life, taking into account the intensification of international flows of personal data subject to automatic processing.[11]

The Convention entered into force for the 47 member states of the Council of Europe and was also ratified and entered into force for Mauritius and Uruguay.[12] The aforementioned treaty aims to guarantee protection in the processing of personal data. It also prohibits the processing of data relating to racial origin, political opinions, religious beliefs, or other beliefs, those relating to health or sexual life and criminal convictions.[13] Individuals are guaranteed the right to know the data stored on them. The only limit to all this is the contrast with a higher interest such as national security or defence.[14] Finally, cross-border flows of data are limited in states where the level of protection is not adequate.

3.2. The European Union and the Protection of Personal Data

Since its foundation, the EU has also placed respect for human rights and the values enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms at the center of its commitments. It is with this in mind that important progress in the field of personal data protection was made in 1995 with the adoption of Directive 95/46 / EC of the European Parliament and of the Council on the protection of individuals with regard to data processing, personal data, as well as the free circulation of such data.[15] This directive aimed to standardize the various data protection regulations between the Member States, an essential requirement to ensure the security of the free movement of data within the EU.

The directive finds its application on data processed by automatic means (such as computer databases) and data in non-automated archives (such as paper).[16] The directive, on the other hand, does not apply to the manipulation of data of a purely domestic or personal nature, and to data used for activities outside the scope of application of Community law, such as defense and public security. The directive establishes the uses for which the processing of data is lawful and, in any case, places the consent of the individual as a necessary requirement. Furthermore, the transfer of data

[10] Lee A. Bygrave, "The 'Strasbourg Effect'on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects." *Computer Law & Security Review* 40 (2021): 105460.

[11] Cécile De Terwangne, "The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data." *International Review of Law, Computers & Technology* 28, no. 2 (2014): 118-130.

[12] Council of Europe, "Chart of Signatures and Ratifications of Treaty 108," Treaty Office. accessed Jan 17, 2021 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=9ylknwkN.

[13] Graham Greenleaf, "'Modernising'data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" *Computer Law & Security Review* 29, no. 4 (2013): 430-436.

[14] Tourkochoriti, Ioanna. "The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance." *U. Pa. J. Int'l L.* 36 (2014): 459.

[15] Paul De Hert, and Vagelis Papakonstantinou. "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals." *Computer law & security review* 28, no. 2 (2012): 130-142.

[16] Dagmar Waldzus, "The European General Data Protection Regulation and Franchise Networks-Time for a Change of Perspective." *Int'l J. Franchising L*. 16 (2018): 12.

to third countries from a Member State has only authorized if the recipient has an adequate level of protection.

Article 28 also provides for the formation of an independent supervisory body for each Member State, which would supervise data protection at the national level: this led to the birth of the national data protection authority. Instead, with Article 29, the Working Party was established, consisting of a representative of each of them and a representative of the commission. Furthermore, the Working Party must inform the Commission in the event of excessive divergence among the Member States laws.[17] It can provide guidance on its own initiative on issues relating to the protection of personal data. Finally, an annual report on the general situation of the protection of personal data processing within the Community shall be drawn up.

Since the effects of the directive were aimed exclusively at States, in 2001 the Data Protection Regulation was formulated by the Community institutions (Regulation 45/2001/EC) in order to extend the protection of personal data also to the processing carried out by bodies and community institutions.[18] In particular, this Regulation establishes the European Data Protection Supervisor (EDPS), a supervisory authority that must evaluate the application of data protection regulations. They can receive complaints from citizens if the latter believe that their right has been infringed by non-compliance with the regulation.[19]

A directive aimed at regulating privacy and electronic communications in a more modern way was approved in 2002. Directive 2002/58/EC specifically regulated the retention of telephone traffic data collected for surveillance purposes by the police.[20] In addition, in the case of breaches that lead to the violation of personal data, suppliers are obliged to send a notification to the national guarantor and in some cases, depending on the type of data compromised, they must also inform the persons concerned.

A further major milestone reached by the EU was the approval of the Charter of Fundamental Rights of the European Union, known as the Treaty of Nice, in 2000. The protection of the right to family and private life is placed within it, in fact, Article 7 states that everyone has the right to respect for his private and family life, his home, and his communications. Subsequently, Article 8 is reserved for the protection of personal data and this is therefore considered a fundamental right of the individual. In the first paragraph of the article, it is stated that everyone has the right to the protection of personal data concerning the person. The second stipulates that such data must be collected on the basis of the principle of justice, for particular justifications, and on the basis of the consent of the individual associated or on any other reasonable grounds provided for by the law. Each individual is entitled to control the data recorded concerning

---

[17] Luca Bolognini, and Camilla Bistolfi. "Pseudonymization and Impacts of Big (personal/anonymous) Data Processing in the Transition from the Directive 95/46/EC to the new EU General Data Protection Regulation." *Computer law & security review* 33, no. 2 (2017): 171-181.

[18] Orla Lynskey, "Data Protection and Freedom of Information; Reconciling the Irreconcilable?" *The Cambridge Law Journal* 70, no. 1 (2011): 37-39.

[19] Lina Jasmontaite, "European Union: The European Data Protection Supervisor (EDPS) Opinion 4/2015 Towards a New Digital Ethics." *Eur. Data Prot. L. Rev.* 2 (2016): 93.

[20] Joel R. Reidenberg, "The Data Surveillance State in the United States and Europe." *Wake Forest L. Rev.* 49 (2014): 583.

him and to obtain its correction. Finally, the third paragraph states that compliance with these rules is subject to the control of an independent authority. The division of the protection of these rights into two specific articles shows the evolution that has occurred in the fifty years following the writing of Article 8 of the ECHR. When the Treaty of Lisbon entered into force on 1 December 2009, the Charter of Nice is included in the form of an annex and thus acquires a legally binding value. According to Article 6 of the Treaty of Lisbon, the Union recognizes the rights, freedoms, and principles enshrined in the Charter of Fundamental Rights of the European Union of 7 December 2000, adopted on 12 December 2007 in Strasbourg, which has the same legal value as the Treaties.

Eventually, in April 2016 the EU Regulation 2016/679 of the European Parliament and of the Council was adopted, the general regulation on data protection (hereinafter GDPR), which came into force starting from 2018, repealing and sending Directive 95/46/EC,[21] which given the exponential technological advances after its establishment and therefore increasingly difficult to adapt to today's world. The Regulation has the great advantage of harmonizing the various national regulations within the European Union, which in the past when transposing Directive 95/46/EC, have sometimes adopted divergent choices. The Regulation is applicable to all data that are processed within the European Union. In addition, it also applies to all data that are processed by non-European subjects, but which process the data of European citizens for the offer of goods and services.

The privacy by design and privacy by default obligations are implemented in the Regulation.[22] In other words, the data controller should adopt internal policies and implement measures that meet in particular the principles of data protection by design and data protection by default. Informing the interested parties and obtaining their consent remains one of the fundamental elements of the Regulation. Furthermore, for particular measures such as "profiling", an impact assessment is required.[23] Individuals must be guaranteed the right to view and correct their personal information. Significant new rights are also established, such as the "the right to be forgotten" and data portability right.[24]

3.3. The United States Personal Data Protection Model

The American model of personal data and privacy protection is completely different from the European, an aspect that sometimes leads to conflicts in transatlantic relations, as for example in the PNR that will be analyzed later. If within the European Union the attempt is that of a strict regulation that limits the manipulation of personal data to what is strictly necessary, the situation in the United States is almost the opposite. American law allows

[21] Malgorzata Magdziarczyk, "Right to Be Forgotten in Light of 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." In *6th International Multidisciplinary Scientific Conference on Social Sciences and Art Sgem 2019*, pp. 177-184. 2019.

[22] Raphael Haganta. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic." *Lex Scientia Law Review* 4, no. 2 (2020): 77-90.

[23] Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR." *Computer law & security review* 34, no. 3 (2018): 436-449.

[24] Eugenia Politou, Alexandra Michota, Efthimios Alepis, Matthias Pocs, and Constantinos Patsakis, "Backups and the Right to be Forgotten in the GDPR: An Uneasy Relationship." *Computer Law & Security Review* 34, no. 6 (2018): 1247-1257.

for a greater invasion of the privacy of its citizens, allowing for a larger collection of data. Furthermore, unlike the European Union, the United States lacks a supervisory authority. Another big difference is the fact that a general law has been adopted within the European Union, first Directive 95/46/EC and the EU Regulation 2016/679, which regulate the processing of personal data in all possible scope and appearance. On the other hand, in the United States, the choice was that of piece-meal legislation, creating a sectoral system.

Without forgetting that the United States, a common law country, protects the right to privacy in an almost exclusively judicial way. The role of the Supreme Court of the United States in the evolution of jurisprudence, which judges in accordance with the Federal Constitution, is therefore fundamental. In the latter, there is no trace of an explicit reference to the right to privacy. However, ad hoc laws are also promulgated to regulate some specific sectors. Also, some of these are federal laws. One of the most important is the Freedom of Information Act (FOIA) enacted in the United States on July 4, 1966.[25] Under that act, it is established that anyone has the right to access the records and archives of federal agencies. It is up to the Government to give explanations in the event that the request for access is refused. In this regard, there are nine exceptions provided for by the act and concern the protection of superior interests, such as respect for privacy or national security.

After that, in 1974, Congress passed the Privacy Act. It was created as a result of the Watergate scandal, in which it became embroiled and even then-President Nixon had to resign.[26] At that time, the absolute need was perceived to put limits on the abuses that were committed by agencies and public bodies against citizens regarding the improper use of information concerning them. Despite the many years that have passed since its adoption, it remains one of the leading privacy protection tools in the United States. However, private subjects are excluded from its field of application, as it only regulates the relationship between citizens and federal government bodies. Furthermore, the Privacy Act only applies to the processing of data belonging to US citizens. Other laws enacted to protect privacy with a very limited scope are for example the Tax Reform Act of 1976 which protected the privacy of financial information, or the Driver's Privacy Protection Act of 1994 which prevented the release of personal information of a driver without consent.

In addition, there is a sectoral privacy approach in which the protection of the citizen is guaranteed with the status of the consumer. There are mainly two possible legal stands. First, according to the principles of fair information practice, in which the fundamental points are the information for the consumer, a request for consent, the possibility of accessing and verifying data, guarantees for the safe storage of data, and measures to respect these principles.[27] Or second with the permissible purpose approach which limits

[25] Ben Wasike, "FOI in Transition: a Comparative Analysis of the Freedom of Information Act Performance Between the Obama and Trump Administrations," *Government Information Quarterly* 37, no. 2 (2020): 101443.

[26] Margaret Hu, "The Ironic Privacy Act," *Wash. UL Rev*. 96 (2018): 1267.

[27] Kuang-Wen Wu, Shaio Yan Huang, David C. Yen, and Irina Popova. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust," *Computers in human behavior* 28, no. 3 (2012): 889-897.

the processing of data to purposes pro-vided for by law.[28] At that point, it is the task of the Federal Trade Commission to ensure that companies comply with the regulations they have adopted and check that there are no unfair practices for consumers. In fact, the right to privacy has poorly protected by this sectoral approach which was further compressed when the Patriot Act was passed in 2001, which greatly expanded the powers of federal agencies, allowing them to access personal information and engage in wiretapping.[29]

4. The Conflict between the US and EU over PNR Codes

Following the US Aviation and Transportation Security Act of November 19, 2001, all airlines departing or arriving in the United States must first send the personal data contained in the PNRs of passengers and crew to the US customs authorities.[30] In this way, the Transportation Security Agency (TSA) can compare these data with government records of individuals at high risk and prohibit people who are dangerous from accessing the aircraft.

There are two methods of data transmission, one is called "push" and the other "pull". With the "push" method, the airlines send the requested data to the databases of the authorities that request them. With the "pull" method, on the other hand, the authorities requesting the data receive free access to their archives from the air carriers and can therefore directly take a copy of the passenger information.[31] At this point, the European airlines found themselves in the cross-fire. On the one hand, the American authorities require to provide the personal data of the passengers, where failure to satisfy the requests could also have led to a ban on landing in the US. On the other hand, there was the European Union legislation that categorically prohibited that transfer.[32] The data of individuals collected for commercial purposes established under Directive 95/46/EC and it prohibited any transfer of data to third countries that do not guarantee an adequate level of protection.

As early as June 2002, the European Commission warned the US authorities that there was a conflict with European data protection legislation, even though it understood the legitimate security interests from which the request for access to PNR originated. The United States took note of this and decided to postpone the entry into force of the new rules until March 5, 2003. From that date on, they would begin to sanction airlines that did not comply with the US Aviation and Transportation Security Act and to since then many large European airlines have begun to give the US authorities access to their PNR

[28] Nancy J King, and V. T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud," *Computer Law & Security Review* 28, no. 3 (2012): 308-319.

[29] Kyle Welch, "The Patriot Act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking," *Cap. UL Rev*. 43 (2015): 481.

[30] Christian Kaunert, Sarah Léonard, and Alex MacKenzie, "The Social Construction of an EU Interest in Counter-Terrorism: US Influence and Internal Struggles in the Cases of PNR and SWIFT," *European security* 21, no. 4 (2012): 474-496.

[31] Noor Huijboom and Gabriela Bodea, "Understanding the Political PNR Debate in Europe: A Discourse Analytical Perspective," *European Politics and Society* 16, no. 2 (2015): 241-255.

[32] Ridha Aditya Nugraha, Dejian Kong, Gaia Guiso, and Lalin Kovudhikulrungsri. "Air and Space Law Education: Preparing for the Future in China, Indonesia, Italy and Thailand." *Hasanuddin Law Review* 7, no. 3 (2021): 183-209.

data.[33] On February 18, 2003, the Commission decided to issue a joint declaration with the US administration, defining the initial requirements for the protection of data operated by US customs, and an agreement to continue negotiations and to ensure that the ways in which US agencies use PNRs are closer to European law, in order to meet the requirements of Article 25 (6) of Directive 95/45/EC regarding adequate data protection transmitted.

In June 2003 the Article 29 Working Party set up by Directive 95/45/EC with tasks of protecting individuals with regard to the processing of personal data, issued a negative opinion, in which they did not consider the guarantee of the States United for the transfer of PNR data to border authorities. First of all, the Working Party's opinion assessed the excessive quantity of information that can be transmitted as compared to what could be considered adequate and relevant, based on Article 6, paragraph 1, letter c of Directive 95/45 / EC. They, therefore, believe that the sending of data should be limited only to some points of the PNR and not to this in its entirety. In particular, sensitive data, protected by article 8 of the directive, should be excluded from sending. In addition to this, the transfer is not considered compatible with the original purpose of the collection. Furthermore, the period of 7-8 years for which the data would be kept is considered too long. According to the Working Party, the data should be removed from the archives after a few weeks, months at most. With regard to data transfer, the only one that complies with the directive is the "push" system in which the airlines provide the American authorities with the data they need. The methods of use of the data are also considered unclear. These should be used to fight against acts of terrorism, while it should not be extended to other serious crimes.

Subsequently, on January 29, 2004, the Working Party reiterated its negative opinion and the presence of critical points in the transfer of PNR to the United States. The new opinion followed a US declaration of commitments and communication from the European Commission intending to reach a bilateral international agreement with the US to authorize airlines to pro-vide PNR data to US agencies. With this opinion, the Working Party, first of all, reaffirmed the principle of finality, therefore PNR can only be used to counter terrorism and cannot also be used for other systems such as CAPPS II. A second point was the principle of proportionality, prohibiting the collection of excessive and irrelevant information.[34] Then once again the importance of conservation was granted for a limited period of time was emphasized. A further point set out the prohibition on processing sensitive data. Finally, there had to be an exercise of the rights of the data subjects. It is necessary that passengers receive clear information about who will use the data collected and for what purposes.

5. The Conflict between the European Commission and Parliament

With Decision 2004/535/EC of 14 May 2004, the Commission granted a protection level to the PNR program in accordance with the requirements required by Directive

[33] M. S. C. Taylor, "Flying from the EU to the US: Necessary Extraterritorial Legal Diffusion in the US-EU Passenger Name Record Agreement." *Spanish Yearbook of International Law* 19 (2015): 221-234.

[34] Douglas Louks, "(Fly) Anywhere but Here: Approaching EU-US Dialogue concerning PNR in the Era of Lisbon." *Ind. Int'l & Comp. L. Rev*. 23 (2013): 479.

95/45/EC.[35] Immediately afterward, by Decision 2004/496/EC, on 17 May 2004, the Council of the European Communities adopted an agreement between the US and the EU on the transfer and processing of PNR data. The European Parliament had expressed itself negatively however in the Council decided it was stated that on the basis of Article 300, paragraph 3 of the Treaty establishing the European Community (TEC).[36] The European Parliament had also sent a request for an opinion on the issue to the Court of Justice of the European Union, registered by the Court Registry on 21 April 2004. However, the Council, fearing a negative opinion, hastened to conclude the agreement and at that point, Parliament had to withdraw its request for an opinion as to the conclusion of the agreement rendered this request devoid of purpose. A few months later, the European Parliament, convinced of the incompatibility of the agreement with the European legislation, presented two further appeals to the Court of Justice on 27 July 2004.

In case C-318/04, which involves the European Parliament v. Commission of the European Communities, the Court should have assessed Decision 2004/535/EC on the adequate protection level in the data transferred to the US border authorities.[37] In case C-317/04 European Parliament v Council of the European Union, it was the objective of the Parliament to obtain the annulment of Decision 2004/496/EC[38] and the consequent careful transfer of PNR to the United States. The rulings of the Court of Justice with regard to the appeals lodged by the European Parliament came in May 2006.

As regards the first case, C-318/04 against the Commission's adequacy decision, the four pleas raised by the Parliament are (1) an excess of power, (2) a violation of the principles of Directive 95/46/EC, (3) a violation of fundamental rights and (4) a violation of the principle of proportionality. First of all, in its judgment, the Court pointed out that according to the second paragraph of Article 3 of Directive 95/46 / EC, cases of transfer of personal data carried out for activities that do not fall within the scope of the law are excluded from its spheres of application towards the community, and in particular those concerning public security, state security, defense, and other activities of the state in the field of criminal law. The Court in its 'recitals' had found that the adequacy decision concerned only the transfer of PNR data to the border authorities of US, Customs and Border Protection, and that this transfer took place under American law. This legislation was aimed at improving the security of the country and regulating entry and exit from the United States.[39]

---

[35] Anna Pateraki, "The Implementation of the Data Retention Directive: A Comparative Analysis," In *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, pp. 317-328. IGI Global, 2011.

[36] Pfisterer, Valentin M. "PNR in 2011: Recalling Ten Years of Transatlantic Cooperation in PNR Information Management," *Nat'l Sec. & Armed Conflict L. Rev*. 2 (2012): 111.

[37] Anna Tsiftsoglou, "Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy," In *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, pp. 93-102. IGI Global, 2011.

[38] Xiana Barros, "The External Dimension of EU Counter-Terrorism: The Challenges of the European Parliament in Front of the European Court of Justice," *European Security* 21, no. 4 (2012): 518-536.

[39] Hassan Syed, "Data Protection Rights & National Security Objectives: Critical Analysis of ECtHR and CJEU Case Law," *North American Academic Research* 2, no. 3 (2019): 155-170.

6. Subsequent PNR Agreements with the US

In July 2007, an agreement was reached between the EU and the US regarding the PNR data transfer, but a response came immediately from Parliament criticizing the legislative process. Subsequently, after the entry into force of the Lisbon Treaty on 1 December 2009, a very important factor changed: the consent of the European Parliament became necessary for the approval of the agreement, and the latter demanded greater attention to the standard protection of data privacy protection. In fact, according to Article 218 of the Treaty on the Functioning of the European Union (TFEU), the approval of the European Parliament was a necessary condition for concluding agreements concerning sectors in which the ordinary procedure applies.[40] Following the abolition of the three-pillar system produced by the Lisbon Treaty, it also includes judicial and police cooperation.[41]

On 5 May 2010, Parliament adopted a resolution postponing the vote which necessary for the approval of the 2007 agreement, in particular, to the attention on safeguarding the right to protection of personal data. [42] The requirements requested by the European Parliament specifically concerned, on the one hand, greater compliance with European legislation on data protection. Then, the need to provide a privacy impact assessment before any measures can be taken in this regard. At the same time, proof of proportionality was necessary to demonstrate the insufficiency of the existing legal instruments. Furthermore, as established by the Framework Decision of 13 June 2002 on combating terrorism, there was to be a strict purpose limitation and use of PNR data limited to crimes or threats assessed on a case-by-case basis. A limitation was also needed regarding the amount of data collected. In its resolution, Parliament also placed a ban on the study of profiles carried out with the extraction of data. Finally, legal supervision and democratic control had to be ensured.

Once negotiations resumed, the Commission proposed a new agreement proposal to Parliament in November 2011. In April 2012 the Parliament was again called to vote on the new revision of the anti-terrorism agreement on the transfer of PNR data and on that occasion the parliamentary majority voted to approve the agreement, despite the negative opinion of the Article 29 Working Party.[43] A significant weight in this decision, in contrast to the choices previously made by Parliament, was undoubtedly that of the political pressure exerted by the United States. The US government had indeed threatened the suspension of visa-free travel to the United States. The new agreement, therefore, took effect on 1 July 2012 and is effective for seven years. The agreement requires the US authorities to keep PNR data in a database for five years. After the first six months, the information with which it is possible to directly identify a passenger is

[40] Hielke Hijmans, "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators," *Eur. Data Prot. L. Rev*. 3 (2017): 406.

[41] Rosanna Belfiore, "The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters," In *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, pp. 355-370. Springer, Berlin, Heidelberg, 2013.

[42] María Quesada Gámez, and Elitsa Mincheva, "No Data Without Protection? Re-thinking Transatlantic Information Exchange for Law Enforcement Purposes after Lisbon," In *EU external relations law and policy in the post-Lisbon era*, pp. 287-312. TMC Asser Press, 2011.

[43] Ángeles Gutiérrez Zarza, "Towards a EU Passenger Name Record (PNR) Scheme?" In *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, pp. 219-222. Springer, Berlin, Heidelberg, 2015.

masked and "de-personalized". At the end of the five years, the data is moved to an “inactive database” for a further ten years, but with stricter access requirements. The purpose of using PNR data must be to combat terrorism and serious transnational crimes.

Previously, the European Data Protection Supervisor (EDPS) had criticized the draft PNR Agreement so that the personal data storage period was shortened considering that it was originally proposed for fifteen years; then the scope of the transferred personal data must also be narrowed and not contain sensitive personal data. PNR should only be used to fight terrorism and transnational crime. In addition, the US Department of Homeland Security may not transfer personal data to other United States authorities or third countries unless they can guarantee the existence of the same level of protection for personal data. EDPS' concerns about threats to EU passenger privacy are not exaggerated given that the United States' positive law, the US Privacy Act of 1974, does little to protect non-citizens. The European Union Commission responded by conducting periodic reviews of its PNR Agreement; and drafting Directive 2016/681/EC56 which came into force on 25 May 2018 to regulate the PNR in more detail for all member countries except Denmark (based on opt-out rights). These regulations will certainly refer to Regulation (EU) No. 697/201657 (General Data Protection Regulation) as applicable on the same date.[44]

7. The New European Directive on PNR

The debate about PNRs reignited sometime later, in particular with reference to the possible threat posed by Europeans who could have returned home after having fought abroad for terrorist groups. In this context, the European Council urged the European Parliament to work swiftly to reach an agreement on a directive on PNR. It also stressed the importance of working with an approach that is consistent with those adopted by third countries, and therefore recommended close cooperation. When the threat of terrorism actually materialized, with the shooting at the Charlie Hebdo headquarters on January 7, 2015, the pressure on Members of the European Parliament to finish work on a directive to govern the transmission and processing of PNR data was intense. In particular, the state heads meeting in Brussels on the following 12 February placed the directive on PNR at the forefront of the most immediate and urgent needs in order to guarantee the safety of citizens.[45]

The 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 offenses and serious crimes was adopted by the European Parliament on 14 April 2016. At the end of the process, the text was approved by the Council of Europe on 21 April and enacted on 27 April.[46] To safeguard the fundamental right to personal data protection, some limitations are placed on the transfer, use, and storage of personal data. Firstly, PNR data can only be processed for investigations in the fight against terrorism or

[44] Ridha Aditya Nugraha. "Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data." *Mimbar Hukum* 30, no. 2 (2018): 262-276.

[45] W. Gregory Voss, "After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy in at Time of Change." *Bus. Law*. 71 (2015): 281.

[46] Birzu, Bogdan. "Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Other Serious Crimes by Using Passenger Name Record (PNR) Data. Critical Opinions. De Lege Ferenda Proposals." *Perspectives of Business Law Journal* 05 (2016): 195-206.

for a serious crime. Secondly, the collection and processing of sensitive data are prohibited. Then, the retention of PNR data is allowed up to a maximum of 5 years, and after an initial period of 6 months, they must be masked and made anonymously, so that the individual cannot be identified directly. Each Member State must create a passenger information unit and must also be transparent and therefore clearly inform passengers of the collection of PNR data. Finally, a transfer of PNR data to third countries has to be assessed on a case-by-case basis.

It, therefore, seems that the striking case of 2012 has been repeated where Parliament voted for political reasons in favor of an agreement that did not meet the requirements it had previously requested. If then it was the US threats that forced many MPs to change their vote, on this occasion, it was the political pressures provoked by the fears that gripped the old continent in the face of the trail of blood started by the attack on Charlie's headquarters and that in the following months-stained other roads in France and Belgium with red. For some, such as the European Data Protection Supervisor, this is an invasive and ineffective measure. In fact, according to the privacy guarantor Buttarelli, in the attacks that took place in the last two years, the information was already available to the authorities and the PNR could not have added anything.[47] In addition to underlining the high costs of the operation and the very long times of the implementation will require. In other words, it can also be concluded that too much information equals no information.

8. Conclusion

The paper elaborates a constantly evolving process, which is still ongoing today. In recent decades, enormous progress has been made in Europe in terms of protecting the right to personal data protection. In particular, the GDPR will undoubtedly make the European privacy law the most advanced in the world. In a world where the exchange of data and information is increasingly massive and fast, it is necessary to protect the data of European citizens even once they have crossed the borders of the Old Continent. In the meantime, until privacy is agreed upon on a global level, Europe has protected itself with Article 25 of Directive 95/46 / EC, which will be replaced by Article 45 of the GDPR.

Terrorism is a significant issue that is becoming even more of a concern every day. It is the issue that hampers the agreement between the EU and the US on PNR data protection. As to protect their national security, the US demands the EU to provide PNR data to their respective agency in order to match with the criminal database. Otherwise, the US will do suspend the EU visa-free travel to the US. The threat of terrorism has created fear in people's souls, and many legislators have been using this apprehension to take extraordinary initiatives that could potentially improve security, and without a doubt diminish privacy. From an economic viewpoint, the relationship between privacy and security has been seen as an exchange among each other. Deciding to enhance security also significantly reduces privacy. Nevertheless, it might be important to regard security as an exception that should be exercised only under specific restrictions. The protection of privacy and other freedoms should always be a primary consideration.

[47] Giovanni Buttarelli, "*Vienna Parliamentary Forum on Intelligence-Security,*" accessed January 4, 2021, https://edps.europa.eu/sites/edp/files/publication/15-05-06_vienna_parliamentary_forum_speech_gb_en.pdf.

References

Barros, Xiana. "The external dimension of EU counter-terrorism: the challenges of the European Parliament in front of the European Court of Justice." *European Security* 21, no. 4 (2012): 518-536.

Belfiore, Rosanna. "The Protection of Personal Data Processed within the Framework of Police and Judicial Cooperation in Criminal Matters." In *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, pp. 355-370. Springer, Berlin, Heidelberg, 2013.

Birzu, Bogdan. "Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Other Serious Crimes by Using Passenger Name Record (Pnr) Data. Critical Opinions. De Lege Ferenda Proposals." *Perspectives of Business Law Journal* 05 (2016): 195-206.

Bolognini, Luca, and Camilla Bistolfi. "Pseudonymization and Impacts of Big (personal/anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulation." *Computer law & security review* 33, no. 2 (2017): 171-181.

Bygrave, Lee A. "The 'Strasbourg Effect'on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects." *Computer Law & Security Review* 40 (2021): 105460.

Council of Europe. (2021). *Chart of Signatures and Ratifications of Treaty* 108. Treaty Office. Accessed Jan 17, 2021, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=9ylknwkN.

Cunningham, McKay. "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law." *Geo. Wash. Int'l L. Rev*. 44 (2012): 643.

De Hert, Paul, and Vagelis Papakonstantinou. "The Proposed Data Protection Regulation replacing Directive 95/46/EC: A Sound System for the Protection of Individuals." *Computer Law & Security Review* 28, no. 2 (2012): 130-142.

De Terwangne, Cécile. "The Work of Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal data." *Int. Review of Law, Computers & Technology* 28, no. 2 (2014): 118-130.

Dutta, Soumitra, Thierry Geiger, and Bruno Lanvin. "The Global Information Technology Report 2015." *In World Economic Forum*, vol. 1, no. 1, pp. P80-85. 2015.

Giovanni Buttarelli, "*Vienna Parliamentary Forum on Intelligence-Security*," accessed January 4, 2021, https://edps.europa.eu/sites/edp/files/publication/15-05-06_vienna_parliamentary_forum_speech_gb_en.pdf.

Greenleaf, Graham. "'Modernising'data Protection Convention 108: A safe basis for a global privacy treaty?." *Computer Law & Security Review* 29, no. 4 (2013): 430-436.

Gutiérrez Zarza, Ángeles. "Towards a EU Passenger Name Record (PNR) Scheme?." In *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, pp. 219-222. Springer, Berlin, Heidelberg, 2015.

Haganta, Raphael. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic." *Lex Scientia Law Review* 4, no. 2 (2020): 77-90.

Hijmans, Hielke. "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators." *Eur. Data Prot. L. Rev*. 3 (2017): 406.

Hu, Margaret. "The Ironic Privacy Act." *Wash. UL Rev*. 96 (2018): 1267.

Huijboom, Noor, and Gabriela Bodea. "Understanding the Political PNR Debate in Europe: A Discourse Analytical Perspective." *European Politics and Society* 16, no. 2 (2015): 241-255.

Jasmontaite, Lina. "European Union: The European Data Protection Supervisor (EDPS) Opinion 4/2015 Towards a New Digital Ethics." *Eur. Data Prot. L. Rev*. 2 (2016): 93.

Ji, Changqing, Yu Li, Wenming Qiu, Uchechukwu Awada, and Keqiu Li. "Big data processing in Cloud Computing Environments." In *2012 12th International Symposium on Pervasive Systems, Algorithms and Networks*, pp. 17-23. IEEE, 2012.

Kaunert, Christian, Sarah Léonard, and Alex MacKenzie. "The Social Construction of an EU Interest in Counter-Terrorism: US Influence and Internal Struggles in the Cases of PNR and SWIFT." *European Security* 21, no. 4 (2012): 474-496.

King, Nancy J., and V. T. Raja. "Protecting the Privacy and Security of Sensitive Customer Data in the cloud." *Computer Law & Security Review* 28, no. 3 (2012): 308-319.

Leetaru, K. (2018). *"What Does It Mean For Social Media Platforms To "Sell" Our Data?,"* https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=240141022d6c.

Louks, Douglas. "(Fly) Anywhere but Here: Approaching EU-US Dialogue concerning PNR in the Era of Lisbon." *Ind. Int'l & Comp. L. Rev*. 23 (2013): 479.

Lowe, David. "The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for Purpose?." *International Criminal Law Review* 17, no. 1 (2017): 78-106.

Lynskey, Orla. "Data Protection and Freedom of Information; Reconciling the Irreconcilable?." *The Cambridge Law Journal* 70, no. 1 (2011): 37-39.

Magdziarczyk, Malgorzata. "Right to be Forgotten in Light of 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." *In 6th International Multidisciplinary Scientific Conference on Social Sciences and Art Sgem 2019*, pp. 177-184. 2019.

Martinez, Ronald, Karon A. Weber, Samantha Tripodi, Winton Davies, Chris Kalaboukis, and Oliver Raskin. "System and Method of Storing Data and Context of Client Application on the web." *U.S. Patent 8,046,437*, issued October 25, 2011.

Newman, Abraham L. "What the "right to be forgotten" means for privacy in a digital age." *Science* 347, no. 6221 (2015): 507-508.

Nugraha, Ridha Aditya, Dejian Kong, Gaia Guiso, and Lalin Kovudhikulrungsri. "Air and Space Law Education: Preparing for the Future in China, Indonesia, Italy and Thailand." *Hasanuddin Law Review* 7, no. 3 (2021): 183-209. http://dx.doi.org/10.20956/halrev.v7i3.3197

Olsen, Henrik Palmer, and Cornelius Wiesener. "Beyond Data Protection Concerns–the European Passenger Name Record System." *Law, Innovation and Technology* 13, no. 2 (2021): 398-421.

Pateraki, Anna. "The implementation of the Data Retention Directive: A Comparative analysis." In *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, pp. 317-328. IGI Global, 2011.

Pfisterer, Valentin M. "PNR in 2011: Recalling ten Years of Transatlantic Cooperation in PNR Information Management." *Nat'l Sec. & Armed Conflict L. Rev*. 2 (2012): 111.

Politou, Eugenia, Alexandra Michota, Efthimios Alepis, Matthias Pocs, and Constantinos Patsakis. "Backups and the Right to be Forgotten in the GDPR: An Uneasy Relationship." *Computer Law & Security Review* 34, no. 6 (2018): 1247-1257.

Quesada Gámez, María, and Elitsa Mincheva. "No data Without Protection? Re-thinking Transatlantic Information Exchange for Law Enforcement Purposes After Lisbon." In *EU External Relations Law and Policy in the Post-Lisbon Era*, pp. 287-312. TMC Asser Press, 2011.

Reidenberg, Joel R. "The Data Surveillance State in the United States and Europe." *Wake Forest L. Rev*. 49 (2014): 583.

Sagiroglu, Seref, and Duygu Sinanc. "Big data: A review." In *2013 International Conference on Collaboration Technologies and Systems (CTS)*, pp. 42-47. IEEE, 2013.

Syed, Hassan. "Data Protection Rights & National Security Objectives: Critical Analysis of ECtHR and CJEU Case Law". *North American Academic Research* 2, no. 3 (2019): 155-170.

Taylor, M. S. C. "Flying from the EU to the US: Necessary Extraterritorial Legal Diffusion in the US-EU Passenger Name Record Agreement." *Spanish Yearbook of International Law 19* (2015): 221-234.

Tourkochoriti, Ioanna. "The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: in Search for Legal Protection Against Surveillance." *U. Pa. J. Int'l L*. 36 (2014): 459.

Tsiftsoglou, Anna. "Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy." In *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, pp. 93-102. IGI Global, 2011.

Voss, W. Gregory. "After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy in at Time of Change." *Bus. Law*. 71 (2015): 281.

Wachter, Sandra. "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR." *Computer Law & Security Review* 34, no. 3 (2018): 436-449.

Waldzus, Dagmar. "The European General Data Protection Regulation and Franchise Networks-Time for a Change of Perspective." *Int'l J. Franchising L.* 16 (2018): 12.

Wasike, Ben. "FOI in Transition: A Comparative Analysis of the Freedom of Information Act Performance between the Obama and Trump Administrations." *Government Information Quarterly* 37, no. 2 (2020): 101443.

Welch, Kyle. "The Patriot Act and crisis legislation: The Unintended Consequences of Disaster Lawmaking." *Cap. UL Rev*. 43 (2015): 481.

Wu, Kuang-Wen, Shaio Yan Huang, David C. Yen, and Irina Popova. "The effect of online privacy policy on consumer privacy concern and trust." *Computers in Human Behavior* 28, no. 3 (2012): 889-897.

Conflict of Interest Statement: The author(s) declares that the research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest.

Hasanuddin Law Review (Hasanuddin Law Rev. – HALREV) is an open access and peer-reviewed journal published by Faculty of Law, Hasanuddin University, Indonesia.

Open Access