EU data protection standards and cooperation agreements with third countries.

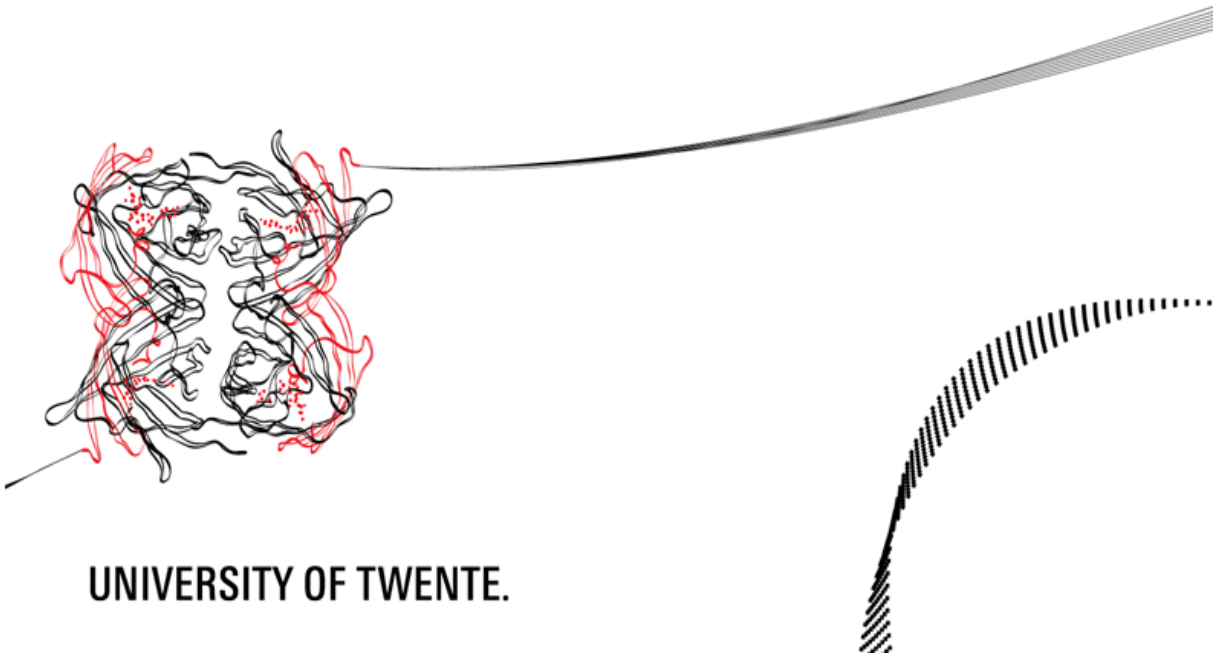
The case of EU–US relations in the Area of Freedom, Security and Justice.

Lisa Schmachtenberg

s1006142
University Twente
Bachelor European Studies

First supervisor: Mr. Claudio Matera
Second supervisor: Prof. Dr. Ramses A. Wessel

20th June 2012, Enschede



List of Abbreviations

AFSJ	Area of Freedom, Security and Justice
CFD	Council Framework Decision 2008/977/JHA
DHS	Department of Homeland Security Privacy Office
EC	European Communities
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EU	European Union
PNR	Passenger Name Record
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
US	United States of America

Table of Contents

Abstract

Over the last years, it became apparent that threats to security have become increasingly transnational in nature. Thus in order to 'prevent, detect, suppress and investigate these threats as well as other criminal offences'[1] the European Union (hereafter: EU) and also its agencies started to conclude agreements on data sharing with third countries, including the United States of America (hereafter: US). However, data sharing may only be permitted if certain EU data protection standards are being protected and, indeed, the EU and its agencies concluded many agreements on data sharing within the Area of Freedom, Security and Justice (hereafter: AFSJ) even though there were no concrete data protection standards available for this area until 2008. Nonetheless, Directive 95/46/EC[2] was the first instrument setting data protection standards within the EU legal order and therefore could have been used and still can be used as a benchmark because of its exhaustive manner in which it regulates the use of personal data.[3]

After describing the data protection principles on the basis of Directive 95/46/EC and other relevant instruments, this study will evaluate the current instrument regulating data protection in the Area of Freedom, Security and Justice – the Council Framework Decision 2008/977/JHA (hereafter: CFD or Framework Decision)[4]– and it will analyse three concluded agreements on data sharing between the EU, its agencies and the United States in terms of their compliance with the EU data protection standards. Accordingly, this study aims at answering the following research question: 'To what extent do the agreements on data sharing of the European Union and its agencies with the United States respect the fundamental data protection standards of the European Union and its member states?'

All in all, this analysis comes to the conclusion that huge differences between the various actors and agreements can be individuated and moreover, it turns out that the agreements are, in fact, not fully in line with the EU data protection standards.

Introduction

Background on data sharing

The abolishment of the internal borders[5] between the member states of the European Union implies not only that ordinary citizens are no longer facing internal border controls but also increases the mobility of criminals. However, 'while the borders are open to criminals, they are still more or less closed to law enforcement agencies due to reasons of national sovereignty'.[6] Therefore, in order to protect national legal systems as well as national sovereignty, member states decided to base the former third pillar,[7] namely police and judicial cooperation in criminal matters, on intergovernmental

[1] For exact wording see: Preamble of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002

[2] Directive 95/46/EC on the on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995

[3] Article 2 of Directive 95/46/EC, OJ L 281, 23.11.1995 'Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'

[4] Council Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008

[5] In 1985, France, Germany, Belgium, Luxembourg and the Netherlands signed the Schengen agreement. This agreement demonstrated the first step towards abolishing the internal borders between the member states of the European Union. For more information see: Nugent (2006). *The Government and Politics of the European Union*. New York: Palgrave Macmillan

[6] For more details see: Kapplinghaus (2007). *Eurojust: Signpost on the road to Security, Freedom and Justice in Europe*. RESOURCE MATERIAL SERIES, No.73, pp.18-28

[7] Until the Lisbon Treaty entered into force in December 2009, the European Union was characterized by a three - pillar structure. The first pillar represented the European Community (EC), the second pillar the Common Foreign and Security Policy (CFSP) and the last pillar was dealing with police and judicial cooperation in criminal matters. While the first pillar was based on supranational cooperation, the second and

cooperation.[8] This is the reason why cooperation in criminal matters, including data sharing, developed slower than under the former first pillar where data sharing had already been disciplined under Directive 95/46/EC in 1995 with the purpose of regulating the free flow of data from one member state to another and establishing the fundamental data protection standards to be respected when personal data is processed.[9]

Indeed, the need to secure privacy when personal data is processed was already recognized in the 1960s when it became obvious that the development of automated data systems and the improvements in digital technology do not only bring advantages, like easier data collection, data processing and transfer –including to third countries– but also disadvantages, like the abuse of data.[10] Since then, securing privacy and accordingly data protection have been of primary concern in the context of European cooperation and, therefore, the first European instrument was adopted by the Council of Europe in 1981.[11] Nevertheless, it took until 1995 for the EU to develop its own instrument and adopt Directive 95/46/EC.

During the 1990s the growing importance of data exchanges was also noticed in security–related matters and thus the introduction of the Area of Freedom, Security and Justice in 1997[12] demonstrated an important step towards more cooperation among the member states in this area. But it was not until the 9/11 terrorist attacks in New York, that the member states realized to further 'speed up the efforts to harmonize national laws, bring down barriers among their law enforcement authorities'[13] as well as to widen and deepen the cooperation at transnational level. Before 9/11, transnational cooperation on data exchange in the fields of policing and criminal law was mainly characterized by bilateral agreements between individual member states of the EU and third states. Against this background, the attacks demonstrated the first moment were 'the European Union expressed its view as a Union on transatlantic cooperation in the fight against terrorism'[14] and extended, for instance, the cooperation with the United States of America. Shortly after the attacks, the US demanded for the conclusion of operational agreements in order to 'prevent, detect, suppress and investigate criminal offences'[15] by sharing personal data between the signing parties. Moreover, apart from the Union itself, also two of its agencies – Europol[16] and Eurojust[17] – concluded agreements on data sharing with the US.

Thus, the EU increasingly started to promote the exchange of data with the US, which consequently resulted in the recognition that this processing needs regulation. However, while Directive 95/46/ EC had indeed established data protection standards, it must be emphasized that Article 3 (2) of the Directive states that that legislation could not apply to the processing of personal data in the field of criminal matters, but exclusively to policies falling within the old pillar.[18] Hence, an instrument was needed in order to establish data protection standards for the AFSJ on the basis of

---

third pillar were based on intergovernmental cooperation. For more information see: Chalmers, Davies & Monti (2010). *European Union Law*. New York: Cambridge

[8] Intergovernmentalism refers to the fact that national governments are the primary actors. These are in charge to decide about European integration. For more details see: Nugent (2006). *The Government and Politics of the European Union*. New York: Palgrave Macmillan

[9] Paragraph (3) of Directive 95/46/EC, OJ L 281, 23.11.1995

[10] For more details see: Birnhack (2008). *The EU Data Protection Directive: An Engine of a Global Regime.* Computer Law & Security Report

[11] Convention 108 for the Protection of individuals with regard to automatic processing of personal data, ETS No.108, 28.01.1981

[12] The Area of Freedom, Security and Justice was introduced with the Amsterdam Treaty in 1997

[13] For more details see: Archick (2011). *US - EU Cooperation against terrorism.* Congressional Research Service

[14] Andreas & Nadelmann (2006). *Policing the Globe: Criminalization and Crime Control in International Relations.* Oxford University Press, p.218

[15] Preamble of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002

[16] Europol (European Police Office) is the European law enforcement agency, which was formally established on July 1st, 1999. For more information see: Fletcher & Lööf (2008). *EU criminal law and justice.* Edward Elgar Publishing, p.76ff

[17] Eurojust is the judicial agency of the European Union that is dealing with criminal matters. It was established on February 28th, 2002. For more information see: Fletcher & Lööf (2008). *EU criminal law and justice.* Edward Elgar Publishing, p.65ff

[18] Article 3 will be discussed more extensively in Part 1.2

existing rules based on Directive 95/46/EC. Indeed, this instrument did not come until 2008 when the Council Framework Decision 2008/977/JHA was finally adopted.

Body of Knowledge

It took several years until the Framework Decision was finally adopted because its negotiation process was characterized by debates and controversies mainly led by the European Parliament, the European Data Protection Supervisor[19] and the Article 29 Working Party.[20] Due to their limited decision–making powers in the former third pillar, their opinions and amendments with reference to the Framework Decision had indeed been heard but were not implemented in the final text.[21] This is why all three actors still argue that the finally adopted Framework Decision is not in line with the fundamental data protection principles of the EU and its member states.[22] Recently, this opinion has received support by many scholars[23] who have critically analysed the Framework Decision in terms of its compliance with the standards set in Directive 95/46/EC. Some of the most significant studies on this topic are the ones by Paul de Hert and Bart de Schutter,[24] Boehm[25] and Els de Busser[26], and, accordingly, there is already some body of knowledge on the evaluation of the Framework Decision. However, until now there is little critical assessment of the impact of the data protection principles on the concluded agreements between the EU, its agencies and the US and that is the reason why this study aims to address the current challenges of the compliance with the data protection principles with a focus on the external dimension of data exchange in the field of police and judicial cooperation.

Research questions

As it was mentioned above, many agreements on data sharing with the US have been concluded by the EU and also its agencies.[27] Those agreements were concluded before 2008 and therefore, during a time were the former third pillar was lacking concrete data protection standards. Taking this into consideration, but bearing in mind the statutory limitation of Article 3, it is nonetheless relevant to understand whether the adopted agreements are in line with the data protection standards contained in

[19] The European Data Protection Supervisor (EDPS) was established by Regulation 45/2001/EC, OJ L 8, 12.01.2001. The EDPS is an independent supervisory body that aims at ensuring that the institutions as well as the agencies of the EU comply with the data protection standards. For more information see: de Hert & Bellanova (2009). *Data protection in the Area of Freedom, Security and Justice: A system still to be fully developed?* Brussels: European Parliament

[20] Article 29 Working Party was established by Directive 95/46/EC. It functions as an independent "advisory body" that is monitoring the compliance with data protection standards. For more details see: de Hert & de Schutter, 2008, p.307

[21] For more details see: de Hert & Papakonstantinouc (2009). *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for*. Computer Law & Security Review, Vol. 25, p.406

[22] For more details see: Tzanou (2010). *The EU as an emerging 'Surveillance Society': The function creep case study and challenges to privacy and data protection*. International Constitutional Law Journal, Vol. 4, pp. 407-427.

[23] The following scholars focused on the evaluation of the Council Framework Decision: de Hert & Bellanova (2009), de Hert & Papakonstantinouc (2009),
Blas (2009). First *Pillar and Third Pillar: Need for a Common Approach on Data Protection?* In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, & S. Nouwt, Reinventing Data Protection? Springer Science and Business Media, pp.225-237
de Hert & Bellanova (2008). *Data Protection from a Transatlantic Perspective: The EU and US move towards an International Data Protection Agreement?* Brussels: European Parliament, pp.1-51
de Hert & Papakonstantinouc (2009). *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for*. Computer Law & Security Review, Vol. 25, pp.403-414.
Hijmans & Scirocco (2009). *Shortcomings in the EU data protection in the third pillar and second pillar. Can the Lisbon Treaty be expected to help*? Common Market Law Review, *Vol.46*, p.1496

[24] de Hert & de Schutter (2008). *International Transfer of Data in the Field of JHA: The Lessons of Europol, PNR and Swift*. Justice, liberty, security: New challenges for EU external relations, pp. 303-340

[25] Boehm (2012). *Data Protection Standards in the AFSJ*. Information Sharing and Data Protection in the Area of Freedom, Security and Justice , pp. 19-173

[26] de Busser (2010). *EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU be Serving its Citizens an American Meal?* Utrecht Law Review, Vol.6, No.1, pp.86-100

[27] The following EU agencies have concluded agreements on data sharing with the US: Europol, Eurojust, The External Borders of the Member States of the European Union (Frontex)

Directive 95/46/EC first and the Council Framework Decision 2008/977/JHA second. Based on this, the following research question emerged:
'To what extent do the agreements on data sharing of the European Union and its agencies with the United States respect the fundamental data protection standards of the European Union and its member states?'

Next to the main research question, three sub–questions have been developed:

(1) What are the fundamental data protection standards of the European Union and its member states?
(2) What is the content of the data protection standards in the Area of Freedom, Security and Justice in comparison to the fundamental data protection standards of the European Union and its member states?
(3) What do the transatlantic agreements on criminal matters between the European Union, its agencies and the United States look like in terms of the fundamental data protection standards?

All research questions can be classified as descriptive research questions. Generally, descriptive studies 'set out to collect, organize and summarize information about the matter being studied'[28] and this holds also true for what this study is aiming to do. Nevertheless, this study cannot be solely classified as being descriptive because it will also analyse the content of the agreements in a comparative manner in order to assess whether they satisfy the standards of the Directive and the Framework Decision and because it analyses which agreement satisfies these standards in the best way.

Methodology

The focus of this study will be on the data sharing agreements with the US only. First, this case selection can be explained by the fact that the US is the most important trade and political partner of the European Union and second, the US is often considered to be the country with the most contested data protection standards that the EU and its agencies are having agreements with.[29] Due to the latter fact, it is reasonable to look first at the contested agreements with the US, before looking at those countries that are having similar data protection standards to those of the EU, like for instance Canada and Switzerland.[30] More precise, this research will focus on the Europol–US,[31] the Eurojust–US[32] and the EU–US agreements on Passenger Name Record (hereafter: PNR).[33]

In fact, all agreements are having the same overall aims, namely to permit data sharing in order to guarantee security while also ensuring the EU data protection standards. In this sense, the comparative case study seems to be the appropriate research design to determine if any differences between the agreements and actors can be observed. The data that will be used for this study will be taken from relevant legislation[34] as well as from research and academic work on the particular topics.[35]

[28] See: Punch (2006) *Developing Effective Research Proposals*. London: Sage, p.33
[29] See: Nino (2010). *The protection of personal data in the fight against terrorism: New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon*. Utrecht Law Review, Vol.6, No.1, p.77
[30] Nino, 2010, p.78
[31] The supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information was signed on December 20th 2002
[32] The agreement between the United States of America and Eurojust was signed on November 6th 2006
[33] The first PNR agreement between the EU and the US was signed in 2004. After much criticism by the European Parliament, the Article 29 Working Party and the European Data Protection Supervisor (Tzanou, 2010) new agreements were concluded in 2006 and 2007. In 2011, the European Commission published a new proposal with the aim to finally satisfy all opponents
[34] Directive 95/46/EC (OJ L 281, 23.11.1995), Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No.5, 04.11.1950), Convention 108 for the Protection of individuals with regard to automatic processing of personal data, (ETS No.108,

Outline of the study

Taking into account the research question as well as the considerations made in this section, this study will be structured as follows: Chapter one will describe the fundamental data protection principles of the EU and its member states based on the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereafter: ECHR),[36] Convention 108 for the Protection of individuals with regard to automatic processing of personal data (hereafter: Convention 108) and Directive 95/46/EC. After identifying the fundamental principles, chapter two will continue with looking at the data protection standards of the Area of Freedom, Security and Justice and will assess whether the latter are in line with the standards set in Directive 95/46/EC and the other instruments. After specifying the similarities and the differences between the various data protection regulations, the third chapter will analyse the agreements concluded between the EU, its agencies and the US and how those look like in terms of the fundamental data protection standards. This study will finish with a conclusion in which, on the basis of the sub–questions, an answer to the main research question will be provided.

Chapter One

1. The data protection principles of the European Union and its member states

During the last decades, digital technology has improved enormously which made the collection as well as the processing of data much easier and faster. Due to the growing importance of data exchanges as well as the recognition of its risks, the EU started to concern itself with the setting up of data protection standards that have to be protected when data is being processed. This chapter will describe the fundamental data protection standards of the EU and its member states based on the ECHR, Convention 108 and Directive 95/46/EC.

1.1. The data protection principles under the ECHR and Convention 108

In 1950, the members of the Council of Europe[37] adopted the *ECHR* and by laying down common standards for the protection of Human as well as Fundamental Rights they aimed at achieving 'greater unity between its members'.[38] It is worth noting that even though data processing and the associated data protection was not a current topic back in the 1950s, it was already recognized as a fundamental right and is since then protected under Article 8 ECHR, namely the right to respect for private and family life:

28.01.1981), Council Framework Decision 2008/977/JHA (OJ L 350, 30.12.2008), Europol – US agreement (December 6th 2001), Eurojust – US agreement (November 6th 2006), EU – US PNR agreement (2004, 2006, 2007, 2012)

[35] In addition to the already mentioned articles by de Hert & de Schutter (2008), Blas (2009), Boehm (2012), Nino (2010), de Hert & Bellanova (2008), de Hert & Bellanova (2009), de Hert & Papakonstantinouc (2009), Tzanou (2010) and de Busser (2010) the following article will especially be taken into consideration:
Brouwer (2011). *Ignoring Dissent and Legality: The EU's proposal to share personal information of all passengers*. CEPS Paper in Liberty and Security in Europe.

[36] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and 14, ETS No.5, 04.11.1950

[37] The Council of Europe was founded in 1949 with the aim of facilitating cooperation among its members (currently 47 members). It is a separate body of the European Union. For more information see: Hix (2005) *The Political System of the European Union*. New York: Palgrace Macmillan

[38] Preamble Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No.5, 04.11.1950

Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

However, over the years, data protection became a topic of concern because the technological advancement made it possible to easily exchange huge amounts of data. The Council of Europe is the most important actor when it comes to the development of data protection principles at the European level[39] and in 1981, its members adopted the first European instrument which aimed at the protection of personal data. This instrument was *Convention 108 for the Protection of individuals with regard to automatic processing of personal data*[40] and it resembles a 'consistent further development of Article 8 ECHR.'[41] Under Article 5, Convention 108 has established five main principles that have to be respected when personal data is being processed: first, the processing must be 'fair and lawful'. Second, data may only be collected for 'specified and legitimate purposes and not used in a way incompatible with those purposes'. In addition to that, the data must be 'adequate, relevant and not excessive in relation to the purposes for which they are stored'. Fourth, personal data undergoing automatic processing shall be 'accurate and kept up to date' and last, the collected data may 'no longer be stored than is required for the purpose for which those data are stored'.[42]

For many years, data sharing was regulated solely by Convention 108. However, because 'the Convention does not regulate the transfer of data to third states', the Council of Europe 'enacted an additional protocol amending Convention No. 108[43] regarding supervisory authorities and transborder data flows.'[44] In fact, this additional protocol did not enter into force before November 2001 and until today only 32 out of the 47 members of the Council of Europe have ratified it.[45]

From the EU perspective, it was only in the 1990s that the European Commission proposed[46] an internal instrument that built upon the five principles established under Convention 108[47] as well as on the provisions laid down in the additional protocol. The proposal of the Commission resulted in the adoption of *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

1.2. The data protection principles under Directive 95/46/EC

In general, Directive 95/46/EC contains the fundamental data protection standards that have to be protected when personal data is processed and, more specifically, nine principles can be identified. On

[39] Boehm, 2012, p.21
[40] Until today 44 out of the 47 member of the Council of Europe have ratified Convention 108. The three countries that have not ratified it are: San Marino, Serbia and Turkey
[41] Boehm, 2012, p.92
[42] For exact wording see: Article 5 of Convention 108, ETS No.108, 28.01.1981
[43] Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001
[44] For exact wording see: Boehm, 2012, p.94
[45] The following EU member states have not ratified the additional protocol amending Convention 108: Belgium, Denmark, Finland, Greece, Italy, Malta, Slovenia and the United Kingdom. The remaining members which have not ratified it are: Azerbaijan, Georgia, Iceland, Norway, Russia, San Marino and Turkey
[46] Proposal from the European Commission *for Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*: OJ No C 277, 05.11.1990 and OJ No C 311, 27.11.1992
[47] Paragraph (11) Convention 108, ETS No.108, 28.01.1981

the basis of previously conducted research[48] it is possible to identify the following principles: (1) the collection principle, (2) the purpose limitation principle, (3) the proportionality principle, (4) the data quality principle, (5) the data retention principle, (6) the data subject principle, (7) the accountability principle, (8) the security safeguard principle and (9) the monitoring or transparency principle.

The first five principles can be found within Article 6 (a) – (e) of the Directive and they mainly incorporated the provisions established under Convention 108. Article 6 begins with the *collection principle* and this first principle refers to the fact that data must be processed in a 'fair and lawful way'.[49] However, before data can be processed, the purposes for the data collection must be specified and according to the second principle, representing the *purpose limitation principle*, data may only be collected 'for specified, explicit and legitimate purposes'.[50] Article 8 adds to that by stating the concrete categories in which data can be transferred. The purpose limitation principle is followed by the *proportionality principle*.[51] This third principle aims at guaranteeing that the collected personal data is 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'.[52] According to principle four, the *data quality principle*, the processed data must be 'accurate and, where necessary, kept up to date'.[53] This includes to check the data upon its correct– and completeness before it is in fact transferred; incorrect as well as incomplete data has to be erased or corrected immediately. Once data has been transferred, the *data retention principle* has to be taken into account. It refers to the time period for which the collected data can be stored and it entails the provision that personal data should be stored for 'no longer than is necessary for the purposes for which the data were collected or for which they are further processed'.[54]

After specifying the conditions under which personal data may be collected and stored, Directive 95/46/EC continues with providing the rights granted to the data subject, laid down in the Articles 10 to 15. Those rights can be summarized under principle six, namely the *data subject principle*, and it basically emphasizes that the individual has a right to be informed when data concerning him/her will be processed. In addition, the individual has been granted the rights to access data[55] as well as to object.[56] The *accountability principle*[57] is principle seven and it regulates that member states are held to be accountable and liable 'when an individual has suffered damage as a result of an unlawful processing operation'.[58] Moreover, principle eight, the *security safeguard principle*[59] deals with the confidentiality and the security of processing. It states that personal data must be protected against 'accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'.[60] Closely connected to the security safeguard principle is principle nine: the *monitoring or transparency principle.*[61] On the one hand, Article 28 entails the important provision that all member states must establish national supervisory bodies which are 'responsible for monitoring the application of the data protection principles within its territory'[62] and on the other hand, Article 29 further develops a 'Working Party on the protection of individuals with regard to the processing of personal data'[63] which

[48] See for instance: de Hert & de Schutter, 2008, p.300ff
[49] Article 6 (a) of Directive 95/46/EC, OJ L 281, 23.11.1995
[50] For exact wording see: Article 6 (b) of Directive 95/46/EC, OJ L 281, 23.11.1995
[51] Article 6 (c) of Directive 95/46/EC, OJ L 281, 23.11.1995
[52] For exact wording see: Article 6 (c) of Directive 95/46/EC, OJ L 281, 23.11.1995
[53] For exact wording see: Article 6 (d) of Directive 95/46/EC, OJ L 281, 23.11.1995
[54] For exact wording see: Article 6 (e) of Directive 95/46/EC, OJ L 281, 23.11.1995
[55] Article 12 of Directive 95/46/EC, OJ L 281, 23.11.1995
[56] Article 14 of Directive 95/46/EC, OJ L 281, 23.11.1995
[57] Article 22 – 23 of Directive 95/46/EC, OJ L 281, 23.11.1995
[58] Article 23 of Directive 95/46/EC, OJ L 281, 23.11.1995
[59] Article 16 and 17 of Directive 95/46/EC, OJ L 281, 23.11.1995
[60] Article 17 (1) of Directive 95/46/EC, OJ L 281, 23.11.1995
[61] Article 28 and 29 of Directive 95/46/EC, OJ L 281, 23.11.1995
[62] For exact wording see: Article 28 (1) of Directive 95/46/EC, OJ L 281, 23.11.1995
[63] Article 29 (1) of Directive 95/46/EC, OJ L 281, 23.11.1995

is an independent advisory body[64] that also monitors the compliance with the data protection principles of the member states. The ninth principle additionally regulates that the Article 29 Working Party as well as the national supervisory bodies have to be informed whenever data is processed[65] and that all processing operations have to be publicized in order to guarantee transparency.[66]

After getting a first impression of the data protection principles, it is important to note two additional articles in order to describe the entire range that is covered by the Directive. First, as it was mentioned in the introduction, this study will exclusively focus on the data sharing agreements with the US. Accordingly, Article 25 of Directive 95/46/EC is particularly relevant because it covers the transfer of personal data to third countries. This provision of the Directive emphasizes that data can only be transferred to a third country if that country guarantees an 'adequate level of protection' of that data. 'The adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations'.[67] In particular, the following considerations should be taken into account: 'the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country'.[68] Nevertheless, it must be pointed out that it is left to the member states to decide if an 'adequate level of protection' is assured.[69] Due to that freedom and the rather vague definition of what is meant by 'adequate', each member state interprets 'the adequate level of protection' in their own individual interest which in reverse brings about chaos across the Union.

The second article that needs to be mentioned is Article 3. This article refers to the scope of Directive 95/46/EC and reads as follows:

Article 3 (2): This Directive shall not apply to the processing of personal data:

> in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

Article 3 thus limits the scope of the Directive to policies falling within the ambit of the old EC Treaty and contains an explicit prohibition of applicability in relation to criminal matters.[70] Therefore, in the light of the abolition of the third pillar, Article 3 (2) must be understood as not being applicable to policies and measures adopted under Title V Treaty on the Functioning of the European Union (hereafter: TFEU)[71] and concerning the 'public security, defence, State security and the activities of the State in areas of criminal law'.[72]

[64] For exact wording see: Article 29 (1) of Directive 95/46/EC, OJ L 281, 23.11.1995
[65] Article 18 – 20 of Directive 95/46/EC, OJ L 281, 23.11.1995
[66] Article 21 of Directive 95/46/EC, OJ L 281, 23.11.1995
[67] Paragraph (56) of Directive 95/46/EC, OJ L 281, 23.11.1995
[68] Article 25 (2) of Directive 95/46/EC, OJ L 281, 23.11.1995
[69] This entails, for instance, that those member states that have bilateral agreements with a certain country argue that an adequate level of protection is given, while those member states without bilateral agreements may argue the opposite. For more information see: de Hert & Papakonstantinouc, 2009, p.412
[70] For exact wording see: Article 3(2) of Directive 95/46/EC, OJ L 281, 23.11.1995
[71] Title V TFEU refers to the Area of Freedom, Security and Justice
[72] For exact wording see: Article 3 (2) of Directive 95/46/EC, OJ L 281, 23.11.1995

1.3. Conclusion of Chapter One

All in all, this chapter has shown that the processing of personal data is covered by a variety of instruments and that the idea behind all those instruments is to ensure the free flow of data while also protecting the fundamental rights of individuals. Here, Convention 108 can be seen as the 'mother instrument'[73] on data protection and Directive 95/46/EC as the more detailed advancement to it.

The description of the data protection principles has illustrated that the Directive not only identifies the characteristics and conditions under which personal data may be processed, but has also illustrated that it grants certain rights to the data subjects, and that it regulates the transfer of data to third states. And exactly the complexity of aspects covered by the Directive makes this instrument so important and advanced. Before the entry into force of the Directive in 1995, Convention 108 was considered to be the main instrument which regulated data sharing. But with the increased transnational cooperation its limitations became apparent because it did not cover the transfer to third states until 2001. Accordingly, there was no single piece of legislation that in fact could cover the technical developments as well as all the aspects that have to be taken into account when data is being shared.

However, this situation changed with the introduction of Directive 95/46/EC. In this sense, the nine data protection standards established under Directive 95/46/EC, can be classified as the fundamental data protection principles of the EU and its member states because, by virtue of their content they aim to be regarded as general principles and as such should be taken into consideration beyond the scope of the Directive. On the other side, the limited scope of the Directive demanded the EU institutions for the adoption of a new instrument that, while based on the same principles, could be tailored to regulate data retention processes and transfer in the different policy fields belonging to the Area of Freedom, Security and Justice and, more precisely, police and criminal law matters.

Chapter Two

2. The data protection principles in the Area of Freedom, Security and Justice

When it was recognized that crime has gained an increasingly borderless character which required the extension of police and judicial cooperation on all levels, the member states agreed upon the development of an instrument that would regulate data sharing in security–related matters. To put this into action, the European Commission prepared a draft proposal for a Council Framework Decision[74] in 2005 that was finally adopted after lengthy negotiations[75] as *Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters* in November 2008.

Taking into consideration the relevance of the principles contained in the Directive, the next section will consider whether the Council Framework Decision is coherent with and founded upon principles similar to the ones of Directive 95/46/EC.

[73] de Busser, 2010, p.88
[74] For more information see: de Hert, & Bellanova, 2008, p.9
[75] For more information see: de Hert & Bellanova, 2008, p.9

2.1. Evaluation of the data protection principles in the Council Framework Decision 2008/977/JHA

The purpose of the Framework Decision is *'to ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy (as reflected in Article 7 and 8 of the Charter of Fundamental Rights of the European Union[76]), with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters'.*[77]

Therefore, Article 1 of the Framework Decision clearly takes over from where the Directive finds its limits as codified in Article 3 (2) and, more specifically, is solely concerned with the processing of personal data in the framework of police and judicial cooperation in criminal matters. Nonetheless, because the Directive embodies general principles related to data protection it seems appropriate to evaluate whether the aforementioned nine principles emerge also from the analysis of the Framework Decision.

The *collection*, the *purpose limitation* as well as the *proportionality* principles have been combined under Article 3 (1) CFD:

Article 3 - Principles of lawfulness, proportionality and purpose

1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes *(purpose limitation principle)* in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful *(collection principle)* and adequate, relevant and not excessive in relation to the purposes for which they are collected *(proportionality principle).*

A closer look at Article 3 (1) CFD suggests that it copies more or less the exact wording of the *collection*, the *purpose limitation* and the *proportionality* principles as provided in Directive 95/46/EC. Nevertheless, Article 3 (1) CFD is distinguishable from the Directive because of the number of exceptions that are not present in the old 'first pillar' instrument. Those exceptions are listed in Article 3 (2)[78] and they permit the processing of data for purposes other than the purposes for which the data was originally collected; for instance, where the 'processing is necessary and proportionate to that other purpose'[79] but at the condition that 'it is not incompatible with the purposes for which the data were collected'.[80] Other exceptions are provided by Article 11 (a)–(d)[81] CFD and in summary, this article permits the further transfer of personal data if it serves 'the prevention, investigation, detection or prosecution of criminal offences'[82] or 'the prevention of an immediate and serious threat to public security.'[83] For 'any other purpose, the transmitting member state or the data subject have to give their prior consent'. [84] These examples have shown that the purposes are defined in such a broad way that further processing is possible for almost any purpose and that in fact all decision–making power is granted to the authorities that are transferring the data. In fact, the Framework Decision grants the status of 'competent authority' non-restrictively to all 'agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police,

[76] Paragraph (48) of Council Framework Decision, OJ L 350, 30.12.2008
[77] Article 1 of Council Framework Decision, OJ L 350, 30.12.2008
[78] Article 3 (2) of Council Framework Decision, OJ L 350, 30.12.2008
[79] Article 3 (2c) of Council Framework Decision, OJ L 350, 30.12.2008
[80] Article 3 (2a) of Council Framework Decision, OJ L 350, 30.12.2008
[81] Article 11 (a) – (d) of Council Framework Decision, OJ L 350, 30.12.2008
[82] Article 11 (a) of Council Framework Decision, OJ L 350, 30.12.2008
[83] Article 11 (c) of Council Framework Decision, OJ L 350, 30.12.2008
[84] For exact wording see: Article 11 (d) of Council Framework Decision, OJ L 350, 30.12.2008

customs, judicial and other competent authorities of the Member States that are authorized by national law to process personal data within the scope of this Framework Decision'.[85]

After illustrating that the first three principles allow for derogations from the fundamental data protection standards, it does not entirely come as a surprise to notice that also the other principles as codified in the Framework Decision have been supplemented with a number of exceptions.

According to Article 4 (1) CFD, 'Personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated' and it could be argued that this wording is appropriate in representing the *data quality principle.* Indeed, its limitations do not become clear until recognizing that it is again left to the authorities that are processing the personal data to decide about the correct– and completeness of the data. Article 4 also regulates the erasure of data and so does Article 5 of the Framework Decision. Indeed in both articles it is argued that data 'shall be stored for no longer than is required for the purposes for which they were lawfully collected (*data retention principle*)'.[86] However, it is interesting to note, with regard to the formulations, that Article 4 as well as Article 5 use the formulation 'shall' while the Directive uses the stronger formulation 'must'.[87] This small distinction, in combination with the fact that 'the purpose may change during the processing,[88] implies that the time limit can easily be adapted to the new purpose'.[89] This is turn means that 'theoretically, the time limit can be indefinitely extended'.[90]

In addition to the regulation of data collection and data processing, the Framework Decision also takes into consideration the rights of the individuals whose data is being processed. Accordingly, the Framework Decision grants the following rights to the *data subject:* the right of being informed, the right of access, the right to object[91] and by Article 19 CFD they have been further given the right of compensation. The right of compensation affirms that member states are held accountable for paying the compensation for the person 'who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions (*accountability principle*)'.[92] In addition to the rights granted to the data subject, Article 21 and 22 of the Framework Decision involve that 'competent authorities must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (*security safeguard principle*)'.[93]

Generally, the Framework Decision uses the same formulations as Directive 95/46/EC when referring to the *data quality*, *data retention*, *data subject*, the *security safeguard* and the *accountability principle.* However, the scope of these provisions appears narrower in the context of the Framework Decision because their applicability is left to the discretion of the competent national authorities[94] not only in relation to the decision on whether to inform the individuals concerned, but also in relation to the measures that they consider to be appropriate in order to protect personal data against abuse. [95] In relation to the *monitoring or transparency principle* it must be emphasized that while the Directive established the 'Article 29 Working Party', which is responsible for monitoring the compliance with the data protection standards of the member states together with the national supervisory bodies, the Framework Decision does not establish its own independent supervisory body but exclusively relies on the national supervisory bodies. These national supervisory bodies 'shall act with complete

[85] Article 2(h) of Council Framework Decision, OJ L 350, 30.12.2008
[86] For exact wording see: Article 4 (2) of Council Framework Decision, OJ L 350, 30.12.2008
[87] Article 6 (e) of Directive 95/46/EC, OJ L 281, 23.11.1995
[88] Refers to Article 3 (2) of Council Framework Decision, OJ L 350, 30.12.2008
[89] Boehm, 2012, p.136
[90] Boehm, 2012, p.136
[91] Article 16, 17 and 18 of Council Framework Decision, OJ L 350, 30.12.2008
[92] Article 19 of Council Framework Decision, OJ L 350, 30.12.2008
[93] Article 22 of Council Framework Decision, OJ L 350, 30.12.2008
[94] Paragraph (27) of Council Framework Decision, OJ L 350, 30.12.2008
[95] Article 22 (1) – (2a – 2j) of Council Framework Decision, OJ L 350, 30.12.2008

independence in exercising the functions entrusted to them'[96] and Article 28 further specifies that previously adopted acts of the Union, like for instance the 'already introduced supervisory bodies, should not be affected by the Framework Decision'.[97] Moreover, Article 1 (2) CFD limits the scope of the Framework Decision to data that 'are or have been transmitted or made available between Member States'.[98] Accordingly, the Framework Decision 'does not include the processing of data that a member states has gathered nationally'[99] and it also explicitly excludes the data processing of the agencies of the EU of its scope.

The following chapter will elaborate this aspect more in detail, but at this point, it is worth briefly mentioning that Europol as well as Eurojust have introduced their own supervisory bodies. And the fact that the Framework Decision does not only leave the supervisory bodies of Europol and Eurojust unaffected but excludes their actions in general of its scope[100] illustrates why the Framework Decision has been criticized for its limited scope. In order to complete this chapter, the 'adequacy principle' will be addressed again. As it was mentioned in the previous chapter, the 'adequacy principle' is rather broad defined and leaves its interpretation, to a large extent, up to the member states. Article 13 (1d) CFD also refers to this principle[101] by stating that 'the third state or international body concerned ensures that an adequate level of protection for the intended data processing'[102] but its assessment criteria[103] are even broader defined than under the Directive. According to paragraph (56) of Directive 95/46/EC, 'the adequacy of the level of protection afforded by a third country *must* be assessed in the light of all circumstances'[104] while under the Framework Decision 'personal data transferred from a Member State to third states or international bodies, should only, *in principle*, benefit from an adequate level of protection.'[105] Furthermore, Article 13 (3) and Article 26 CFD permit derogations from Article 13 (1d) for instance in the case where the EU or one of its member states has already concluded a previous agreement with the third state.[106]

2.2. Conclusion of Chapter Two

The Framework Decision was the long waited for instrument that would apply the principles established under Directive 95/46/EC and accordingly regulate the data protection in the former third pillar. Nevertheless, its adoption was characterized by a long process of negotiations. On the one hand, the member states recognized the need for the establishment of an appropriate instrument in the Area of Freedom, Security and Justice but on the other hand, they wanted to protect their sovereign power in police and judicial cooperation. This conflict resulted in the fact that the Framework Decision now rather represents an agreement consisting of compromises, which becomes especially obvious by focusing on the broad definitions and formulations used in the Framework Decision. While Directive 95/46/EC almost continuously uses the formulation 'must' in order to demonstrate the importance of the principles, the Framework Decision sticks to weaker formulations like 'shall' and 'in principle'.[107] Furthermore, the Framework Decision allows for broad derogations from the fundamental data protection principles; this phenomenon can be observed throughout the entire Framework Decision.

[96] Article 25 of Council Framework Decision, OJ L 350, 30.12.2008
[97] de Hert & Papakonstantinouc, 2009, p. 413
[98] Article 2 (a) of Council Framework Decision, OJ L 350, 30.12.2008
[99] de Busser, 2010, p. 90
[100] Paragraph (39) of Council Framework Decision, OJ L 350, 30.12.2008
[101] Paragraph (23) of Council Framework Decision, OJ L 350, 30.12.2008
[102] Article 13 (1d) of Council Framework Decision, OJ L 350, 30.12.2008
[103] Article 13 (4) of Council Framework Decision, OJ L 350, 30.12.2008
[104] Paragraph (56) of Directive 95/46/EC, OJ L 281, 23.11.1995, emphasis added.
[105] Paragraph (23) of Council Framework Decision, OJ L 350, 30.12.2008, emphasis added.
[106] Article 26 of Council Framework Decision, OJ L 350, 30.12.2008
[107] Paragraph (23) and (24) of Council Framework Decision, OJ L 350, 30.12.2008

In relation to the substance, the Framework Decision refers to all nine fundamental data protection principles as introduced by Directive 95/46/EC. However, when having a closer look at the principles it becomes apparent that each principle 'had been tied to exceptions that made their application in practice uncontrollable'.[108] In addition, the Framework Decision did not establish its own independent supervisory body which monitors the compliance with the data protection standards in the Area of Freedom, Security and Justice but almost all decision–powers are left to the member states and their competent authorities. The combination of member states and their authorities is often considered of not resulting in an overall accountable and transparent system in which data, relevant for the fields of the Area of Freedom, Security and Justice, is retained and processed.

The abovementioned aspects led to the conclusion, that the data protection principles established under the Framework Decision cannot be considered to be equivalent to those established under Directive 95/46/EC. Rather, the Area of Freedom, Security and Justice 'consists of a patchwork of different applicable rules making it difficult to illustrate the data protection instruments and principles in this area'.[109]

Chapter Three

3. The data protection principles within the concluded agreements on criminal matters between the European Union, its agencies and the United States

The analysis carried out in the previous chapters has illustrated that the principles established under Directive 95/46/EC should be considered as the fundamental data protection principles of the European Union and its member states. However, it has also emerged that the data protection principles established in the Area of Freedom, Security and Justice cannot be constructed as representing a consistent development or a mere projection of those principles in the AFSJ context because the Framework Decision seems to purposively depart from the principles adopted in the Directive.

This study has frequently referred to the 'adequacy principle' because of its importance in relation to the nine fundamental data protection principles and because of the role this principle has in external relations. Therefore, this element will be addressed in this chapter. In this perspective, it is worth noting that the 'European Commission has not found that the US as a whole ensures an adequate level of protection.'[110] Accordingly, it is left to European authorities to decide, on a case–by–case basis, if the US is *concretely* guaranteeing an adequate level of protection. Furthermore, the US is considered to be different from the EU in the following aspects with regard to data protection: first, the US does not have a 'general framework concerning the processing of personal data'[111] and second, the independent US data protection authority, the Department of Homeland Security Privacy Office (hereafter: DHS), is defined 'as not structurally independent when compared to EU data protection authorities'.[112] Against this background, Europol, Eurojust and the Union itself have concluded agreements in criminal matters with the US. In the light of the substantive limits of the Framework Decision on the one side, and taking into consideration that the two agencies as well as the EU have concluded agreements on the matter even before there was an instrument on data protection available in the former third pillar, this section will examine whether these agreements with the US can be

[108] de Hert & Papakonstantinouc, 2009, p. 407
[109] Boehm, 2012, p. 107
[110] Opinion of the European Data Protection Supervisor, 09.02.2012
[111] For exact wording see: Nino, 2010, p.77
[112] de Hert & Bellanova, 2008, p.20

considered to be consistent with the fundamental data protection principles emerged from the Directive before looking at the consistency with the Framework Decision.

3.1. Evaluation of the operational agreements between Europol, Eurojust and the United States

Before analyzing the agreements between the US and the European agencies, it is important to mention the objectives and rules that are regulating the processing of personal data of Europol and Eurojust.

Europol was created by the Europol Convention adopted in 1995 under the former third pillar of the Maastricht Treaty and its objectives are 'preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime where there are factual indications that an organized structure is involved'.[113] While Europol aims at encouraging law enforcement cooperation in criminal matters as well as enhancing police investigations, Eurojust was created by Council Decision 2002/187/JHA in order 'to improve judicial cooperation between the Member States further, in particular in combating forms of serious crime often perpetrated by transnational organizations'.[114] However, both agencies were brought within the legal framework of the EU and their activities are now regulated by newly adopted instruments; since November 2008, the activities of Eurojust are regulated by *Council Decision on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*[115] and the current instrument regulating the activities of Europol is *Council Decision adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information*[116] which was adopted in November 2009.

As it was mentioned in the first chapter, because of the importance of Convention 108 and the codification of the five main principles related to the processing of data, this instrument has been used as a reference by the two agencies since their establishment. Therefore, due to the sensitiveness of the activities carried out by the two agencies, data protection has been considered as a topic of huge importance for the purposes of their actions and, as a consequence of this, both founding instruments contain an express reference to the five principles of Convention 108.[117]

Moreover, the founding instruments of the two agencies go beyond the Convention's principles and grant individuals the right of access to personal data[118] as well as establish independent Joint Supervisory Bodies[119] which "ensure that the processing of personal data is carried out in accordance with" [120] the newly adopted Council Decisions. In addition, both contain provisions which regulate the processing to third states and international organizations.[121] These provisions impose the 'adequate requirement as a prerequisite for data transfer to a third state'.[122] Overall, it can be said that Europol as well as Eurojust have developed their own very detailed provisions that regulate the processing of personal data, but that both systems can be seen as developments stemming from the principles and rules contained in Convention 108 and Directive 95/46/EC. By emphasizing that, we can continue with analyzing how these provisions are implemented in the agreements with the US.

---

[113] Article 2(1) of the Europol Convention, OJ C 316, 27.11.1995
[114] Preamble 1 of Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[115] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 138, 04.06.2009
[116] Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, OJ L325, 11.12.2009
[117] Article 14 of the Europol Convention, OJ C 316, 27.11.1995 and Article 14 (2) – 25 of the Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[118]Article 19 of the Europol Convention, OJ C 316, 27.11.1995 and Article 18 and 19 of the Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[119]Article 24 of the Europol Convention, OJ C 316, 27.11.1995 and Article 23 of the Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[120] Article 23 (1) of Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[121] Article 18 of the Europol Convention, OJ C 316, 27.11.1995 and Article 26 (a) of Council Decision 2002/187/JHA, OJ L 63, 06.03.2002
[122] de Busser, 2010, p.96

After the 9/11 terrorist attacks, states increased the transnational cooperation in order to prevent such a terrorist attack from happening again. Resulting from this fact, Europol and the US signed an agreement with the purpose to 'prevent, detect, suppress, and investigate criminal offences, in particular by facilitating the reciprocal exchange of information, including personal data'[123] in December 2002. Even though, the agreement considers that it is in their 'common interest to extent their cooperation to, inter alia, the exchange of personal data, with the regard to the rule of law and protection of individuals rights and liberties'[124] the introduced provisions that should guarantee the protection of these rights and liberties are formulated very broadly and often lack a clear definition. For instance, Article7 affirms that 'information shall be available to competent U.S. federal authorities'[125] but the agreement does not define what is meant by 'competent' and further, 'the US was unable to give Europol a list of authorities that would be eligible to receive data in accordance with this agreement'.[126]

Furthermore, the agreement is only referring to two of the fundamental data protection principles: While Article 9 is very much in line with maintaining the accuracy of information (*data quality principle*) as provided by Directive 95/46/EC, the provisions under Article 5, concerning the *purpose limitation principle*, are rather limited. Article 5 implies that the receiving party must specify the purposes for which the data will be used, but the Article further implies that 'where the receiving Party seeks the use of such information for other purposes' it only has to 'ask for the prior consent of the Party that furnished the information'.[127] However, the remaining principles[128] that compose the body of data protection rules within the EU are not dealt with in the concluded agreement.

So far, the analysis of the agreement between Europol and the US has given rise to the assumption that Europol has 'ignored its own data protection provisions'.[129] Nevertheless, this assumption does not apply to the agreement that was signed between Eurojust and the US in November 2006. Its purpose is to 'enhance cooperation between the two in combating serious forms of transnational crime including terrorism'.[130] After providing the purpose, the scope and the authorities who are competent for the execution of the agreement, the agreement continues with the authorization to exchange data and the data protection rules in Article 8, 9 and 10. In principle, these three articles refer to the five data protection principles developed under Convention 108.[131] Besides referring to these principles, the agreement also ensures the protection of the four additional protection principles established under Directive 95/46/EC by protecting 'personal data against accidental or unlawful destruction, accidental loss or unauthorized disclosure, alteration, access or any authorized form of processing',[132] 'granting individuals access to personal data[133] as well as the possibility to correct, block and delete personal data relating to him/her'.[134] Last, the oversight of implementation as well as the compliance with the agreement is to be controlled by 'respective administrative, judicial or

[123] For exact wording see: Article 1 of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002
[124] Preamble of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002
[125] For exact wording see: Article 7 (1a) of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002
[126] de Busser, 2010, p.97
[127] Article 5 (1a) of the supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information, 20.12.2002
[128] The remaining principles are: The collection, the proportionality, the data retention, the data subject, the accountability, the security safeguard and the transparency principle. For more details see: Directive 95/46/EC, OJ L 281, 23.11.1995
[129] de Busser, 2010, p.96
[130] Article 2 of the Agreement between the United States of America and Eurojust, 06.11.2006
[131] Agreement between the United States of America and Eurojust, 06.11.2006: Article 8 in combination with Article 19 deals with the purposes under which data may be processed. In addition, Article 9 contains the provisions that the processing must be fair, data must be adequate and relevant in relation to the specific purpose, it must be stored for no longer than is necessary and last, the data must be accurate.
[132] Article 13 of the Agreement between the United States of America and Eurojust, 06.11.2006
[133] Article 15 of the Agreement between the United States of America and Eurojust, 06.11.2006
[134] Article 16 of the Agreement between the United States of America and Eurojust, 06.11.2006

supervisory bodies that will ensure an appropriate level of independence of the oversight process'.[135] All in all, the agreement between Europol and the US does not contain as detailed and far reaching provisions as provided in the Eurojust–US agreement and in this respect, one might wonder the extent to which it is legitimate for Europol to depart from its own statute in its external relations.

3.2. Evaluation of the EU–US agreements on Passenger Name Records

Until today, four agreements on Passenger Name Records[136] have been concluded between the EU and the US with the aim to 'prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and common values'.[137] Before continuing with the analysis, it is worth to shortly summarize the developments of the PNR agreements. [138]

In May 2004, the first agreement on PNR was signed within the first pillar. After the European Court of Justice had ruled that it did not fall within the field of competences of the first pillar but the third one, an interim agreement was signed in 2006 in order to replace the agreement of 2004. Indeed, the interim agreement expired in 2007 which required the adoption of a new agreement in 2007. Ever since the first agreement on PNR between the EU and the US entered into force, the European Parliament and the Article 29 Working Party have argued that the agreements are 'in complete violation of principles provided by Directive 95/46/EC, Article 8 of the ECHR, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union'.[139] Due to rising criticism as well as the long list of amendments provided by the European Parliament and the Article 29 Working Party, the 'European Commission published a proposal for a new directive on the use of PNR data in 2011'.[140] However, the European Parliament did not give its consent to the Commission's proposal until April 2012. After the European Parliament gave its consent, the 'Council adopted a decision on the conclusion of a new EU–US PNR agreement which will replace the existing one, provisionally applied since 2007. This agreement will most likely enter into force on 1 June 2012'.[141]

After briefly illustrating the reasons which constantly led to the development of new PNR agreements, this study will analyse whether the criticism raised seems convincing or whether it is possible to conjugate the wording of the agreements with the principles of Convention 108 and the Directive. Taking into account the PNR agreements concluded in 2007 and 2012, this analysis will provide a systematic analysis of the two agreements.

Indeed, both agreements 'explain how the United States Department of Homeland Security handles the collection, use and storage of PNR'[142] and on the basis of these explanations it is possible to evaluate the agreements in terms of its compliance with the fundamental data protection.

Firstly, in relation to the scope of the agreements, both texts affirm that the purposes for which the DHS will use PNR data are to 'prevent, detect, investigate and prosecute: (1) terrorist offenses and

---

[135] Article 19 of the Agreement between the United States of America and Eurojust, 06.11.2006

[136] *First Agreement:* Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20.05.2004. *Second Agreement*: Agreement between the European Union and the United States of America on the processing and transfer of passenger name records (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298, 27.10.2006. *Third Agreement:* Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR agreement) OJ L 204, 04.08.2007. *Fourth Agreement*: 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, Council of the European Union, 17434/11

[137] 2007 PNR agreement, OJ L 204, 04.08.2007

[138] For a detailed summary of the PNR agreements see for instance: Geyer (2008). *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*. Challenge Liberty and Security, Vol.9, p.32

[139] Nino, 2010, p.71

[140] Brouwer, 2011, p.1

[141] Council of the European Union: Council adopts new EU – US agreement on PNR data, 9186/12, PRESSE 173, 26.04.2012

[142] For exact wording see: First paragraph of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007

related crimes and (2) other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature'.[143] The formulation 'other crimes' is rather vague and includes that data could be processed for nearly any purpose. Therefore, while this Article should have served the purpose of defining and thus limiting the scope of applicability of the agreement in relation to the exchange of data, it appears that the formulation is not about '*purpose limitation* and, rather, about purpose deviation'.[144] The same phenomenon of deviation can be observed for the *proportionality principle*. Here, the DHS can require the collection of 19 types of information[145] and in 'an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired, DHS officials may require and use information in EU PNR other than those listed above, including sensitive data'.[146] Another provision which aroused criticism is the one relating to *data retention*. Under the PNR agreement of 2004 it was possible to access PNR data for a period of three years and six months and under the PNR agreements of 2007 and 2012 this period has increased to 15 years.[147] First, 'PNR can be retained in an active database for up to five years and after this active period, PNR shall be transferred to a dormant database for a period of up to ten years'.[148] This excessive provision does not only contradict the *data retention principle* but also the *proportionality principle*. The agreements continue with specifying that the 'EU PNR data is treated as sensitive and confidential in accordance with U.S laws'.[149] At first view, this wording could be considered to be in line with the *collection principle*. However this impression changes when becoming aware of the fact that the agreement does not take 'into account the existence of differences between Community law and US laws regarding the processing of personal data'.[150] A huge difference is, for instance that the 'protection of personal data is not recognized as a constitutional right in the US'.[151] Moreover, the DHS aims at promoting greater transparency by 'providing information to the travelling public about its processing of PNR data through publications in the Federal Register and on its website'.[152] Nevertheless, none of the agreements established an independent supervisory body which monitors the compliance with the agreed upon data protection principles.

So far, the two agreements follow the same pattern with regard to the compliance with the data protection principles, however the following two aspects will illustrate that the 2012 PNR agreement is more advanced in terms of data protection than the PNR agreement of 2007. Firstly, while the 2007 PNR agreement does not particularly refer to the *data subject*, *the data quality*, *the security safeguard* and the *accountability* principles, the 2012 PNR agreement has incorporated the *data subject*[153], the *security safeguard*[154] as well as the *accountability*[155] principles. According to the *data subject* principle, individuals have a right of being informed when data concerning him/her will be processed and even though the 2012 PNR agreement does not contain this provision, individuals have

[143] Article 4 of the 2012 PNR agreement
[144] For exact wording see: de Busser, 2010, p.97
[145] 1. PNR record locator code, 2. Date of reservation/issue of ticket, 3. Date(s) of intended travel, 4. Name(s), 5. Available frequent flier and benefit information (i.e. free tickets, upgrades, etc.), 6. Other names on PNR, including number of travelers on PNR, 7. All available contact information (including originator information), 8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction), 9. Travel itinerary for specific PNR, 10. Travel agency/travel agent, 11. Code share information, 12. Split/divided information, 13. Travel status of passenger (including confirmations and check-in status), 14. Ticketing information, including ticket number, one-way tickets and Automated Ticket Fare Quote,15. All baggage information, 16. Seat information, including seat number, 17. General remarks including OSI, SSI and SSR information, 18. Any collected APIS information, 19. All historical changes to the PNR listed in numbers 1 to 18
[146] Title III. of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007 and Article 6 (3) of the 2012 PNR agreement
[147] Title VII. of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007: DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and Article 8 of the 2012 PNR agreement
[148] For exact wording see: Article 8 (1) – (2) of the 2012 PNR agreement
[149] Title II. of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007
[150] Nino, 2010, p.77
[151] Geyer, 2008, p.45
[152] Title VI. of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007 and Article 10 of the 2012 PNR agreement
[153] Article 11 and 12 of the 2012 PNR agreement
[154] Article 5 of the 2012 PNR agreement
[155] Article 13 of the 2012 PNR agreement

at least been granted the right of access[156] and the 'right of correction or rectification, including the possibility of erasure or blocking'.[157] Furthermore, in the case that 'personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law (*accountability principle*)'.[158] And lastly, the 'DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing or use (*security safeguard* principle)'.[159] Indeed, the analysis of these three principles leads to the conclusion that they are predominantly in line with the data protection standards established by Directive 95/46/EC. The only principle that is still not dealt with in the newly adopted PNR agreement is the *data quality* principle. Secondly, another striking feature of the 2007 PNR agreement held that the DHS required in turn for ensuring 'an adequate level of protection of PNR data transferred from the EU, that the EU will not interfere with relationships between the US and third countries for the exchange of passenger information on data protection grounds'.[160] However, this contested provision has been removed and the 2012 PNR agreement replaced it by introducing the provision that the 'DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing'.[161]

3.3. Conclusion of Chapter Three

As a conclusion for this chapter it can be said that the analysed agreements present important differences in relation to the compliance with the fundamental data protection principles.

In fact, Europol and Eurojust have implemented the fundamental data protection principles within the former third pillar by making them applicable and part of their own data protection principles. Yet, when it comes to their implementation it is questionable why especially these two actors, which developed nearly identical data protection principles, differ so much with regard to the concluded data sharing agreements with the US. More precisely, while Eurojust complies with its own principles and is in accordance with the fundamental data protection principles also when concluding agreements, Europol does not seem to do the same. However, the fact that Eurojust and Europol recognized the principles established under Directive 95/46/EC as the fundamental data protection principles does not entail that they have been recognized as such in the entire third pillar and this became apparent by evaluating the EU–US agreement on PNR. While the Europol–US as well as the Eurojust–US agreement very highly welcomed from the beginning on, the EU–US agreement on PNR already had a difficult start and has continued to be a contested agreement.

In the light of the foregoing, it cannot be doubted that the 2007 agreement was sealed under the dominant political will of the US and that the EU has not been capable of declaring its trust to the level of protection of personal data declared by the US government and the assessment of the 2012 PNR agreement has shown that this situation has not changed until today. Indeed, the assessment of the EU–US agreements on PNR arrives at the conclusion that the PNR agreement concluded in 2012 is more advanced in terms of data protection than the 2007 PNR agreement. But after taking into consideration that the new agreement is still not in line with the fundamental data protection principles with reference to the *purpose limitation*, the *proportionality* and the *data retention* principles, it

[156] Article 11 of the 2012 PNR agreement
[157] Article 12 of the 2012 PNR agreement
[158] Article 13 of the 2012 PNR agreement
[159] Article 5 (4) of the 2012 PNR agreement
[160] For exact wording see: Paragraph 6 of the US letter to EU in the 2007 PNR agreement, OJ L 204, 04.08.2007
[161] Article 19 of the 2012 PNR agreement

becomes obvious that the EU still does not manage to convince the US of the application of their data protection standards.

Moreover, the evaluation of the EU–US PNR agreements and the Europol–US agreement gets predominantly to the same result and concludes that the EU and also Europol have signed the agreements with the US even though they are aware of the fact that these are not respecting the fundamental data protection principles of the EU and its member states.

Conclusion

The extent to which transatlantic agreement on criminal matters between the European Union, its agencies and the United States respect the fundamental data protection principles

As the international transfer of personal data increased, the Framework Decision 'was supposed to be celebrated'[162] as the data protection instrument for security–related matters equivalent to Directive 95/46/EC. But *'the EU legal framework in the Third Pillar can be best defined as a patchwork of data protection regimes. There is no legal framework which is stable and unequivocal, like Directive 95/46/EC in the First Pillar*'.[163] And although this statement refers to the situation of the former third pillar, it is still valid until today.

The analysis carried out in this study has emphasized the importance of the principles established under Directive 95/46/EC and therefore, it could be argued that the Directive despite Article 3 (2) can be considered as *acquis* of the Union.[164] This legally justifies the use of the Directive as a benchmark for the application of the data protection principles. In particular, its importance can mainly be observed at two facts. First, they cover a variety of aspects that have to be protected when data is being shared and second, even though the principles only apply to Community matters the member states have implemented them in other areas where no equivalent data protections standards are available as well.[165] Here, Europol and Eurojust can be used as good examples. Moreover, this assumption seems reinforced with the entry into force of the Lisbon Treaty and the EU Charter of Fundamental Rights.[166]

Due to the fact that the Framework Decision was not adopted until 2008, Europol and Eurojust had to develop their own provisions that would regulate data sharing. In fact, both made the principles developed under the Directive to their own data protection principles. Being aware of this fact, the assumptions arises that the concluded agreements with third states, and here in particular with the US, may be in line with the fundamental data protection principles even though at the time of conclusion there was no standard–setting text regulating data sharing particularly in security–related matters. But the forgoing evaluation of the transatlantic data sharing agreements with the US comes to rather mixed results concerning this assumption. In particular, the extent to which the agreements on data sharing of the European Union and its agencies with the US respect the fundamental data protection standards of the European Union and its member states is different for each of the evaluated agreements.

More precisely, the Europol–US agreement only refers to two out of the nine fundamental data protection principles and it generally contains too many open formulations. Eurojust on the contrary

[162] de Hert & Papakonstantinouc, 2009, p.405
[163] Hijmans & Scirocco, 2009, p.1496
[164] 'The acquis is the name of the existing body of law that the European Union and its member states have been adopted until now'. For more information see: Chalmers, Davies & Monti, 2010, p.28
[165] For more details see: Blas, 2009, p.231
[166] Here Article 16 Treaty on the Functioning of the European Union is of huge importance

applies all nine principles and in addition to that, its data supervisory regime is said to be very effective; 'the internal supervision is carried out by the Data Protection Officer and externally by the Joint Supervisory Body. Their members are to be nominated by the member states and the aim of the internal as well as the external supervisory authority is to ensure that the processing of data is carried out in accordance with the Eurojust decision'[167] and thus the fundamental data protection principles. Although Europol and Eurojust share the opinion that data protection is of huge importance, the assessment has shown that they deal differently with the implementation of the fundamental data protection principles.

So far we have only taken into consideration the agreements between the US and the agencies of the EU but what about the PNR–agreements concluded by the EU itself? As a general fact, it must be said that over the years increasingly more fundamental data protection principles were incorporated in the agreements concluded on PNR. Thus, the 2012 PNR agreement incorporated the fundamental data protection principles to the largest extent. At this point it could be argued that the Europol–US and the EU–US agreements on PNR are weaker than the Directive in terms of data protection but, in fact, compatible with the Framework Decision. This compatibility becomes apparent by recognizing that the Framework Decision and the agreements are similarly handling the following aspects: First, the *collection*, the *purpose limitation* and the *proportionality* principles are included but they are either defined very broad or tied to derogations. And secondly, they accept that the 'US opposes to define an appropriate retention period'.[168] However, these similarities account at the same time for the conclusion that the principles developed under the Framework Decision cannot be considered to be equivalent to the fundamental data protection principles established under the Directive.

As argued above, the core elements of the Directive must be understood as acquis of the EU legal order and regardless of the fact that the Framework Decision and the agreements are compatible with one another, the evaluation of the Framework Decision has identified its limitations and thus, the two agreements are in breach of the fundamental data protection principles contained in Directive 95/46/EC.

Overall no general pattern among the transatlantic agreements on criminal matters between the US, its agencies and the US with regard to the fundamental data protection principles of the EU and its member states can be observed. While the Europol–US agreement and the EU–US agreement on PNR are more or less disrespecting the fundamental data protection principles, the agreement between Eurojust and the US illustrates that it is possible to cooperate while also protecting its own data protection principles. Generally, 'data protection has been and will continue to be a key EU–US striking point'[169] if the US will not guarantee a better and more transparent protection of the European personal data. The EU as well as the US are interested in a well functioning cooperation but currently, the EU it making too many compromises at the expense of its citizens with regard to the data sharing agreements with the US. Only if the EU will stronger demand for the application of their standards and only if the US is willing to protect personal data stricter, then the cooperation between the two is likely to remain successful.

Taking into account the divergences from this analysis, the next question would be to assess the factors that lead to the differences. Yet, while a comprehensive answer to this question would go beyond the scope of this study, one potential element need to be mentioned. This potential element is that there is 'no comprehensive data protection scheme available that covers all areas of EU

[167] For exact wording see: Blas (2010). *Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom.* ERA Forum, Vol.11, p.247
[168] For exact wording see: de Hert & Bellanova, 2011, p.5
[169] For exact wording see: Archick, 2011, p. 6

competence'[170] and that data protection is rather characterized by various pieces of legislation which are all different in their extent in complying with the fundamental data protection principles.

As it has been argued, the impact of lacking a comprehensive data protection scheme can clearly be felt within the Area of Freedom, Security and Justice. Here, data protection is on the one hand regulated by the Framework Decision and on the other hand, by case–specific legislation developed by Europol and Eurojust which are in fact operating independent from the Framework Decision.

Regardless of the fact if it would turn out to be an explaining factor or not, the Lisbon Treaty[171] now offers the possibility for change. The entry into force of the Lisbon Treaty has led to some important changes for the Area of Freedom, Security and Justice and, more precisely, for the future of data exchange within the EU and with third countries.

The assessment of the Framework Decision has indeed demonstrated its limitations in terms of the compliance with the fundamental data protection principles and this is not least due to the limited involvement of the European Parliament in its adoption process. Under Lisbon, the European Parliament has been granted more decision-making power in the AFSJ and because the European Parliament is very 'mindful of the protection of the rights and fundamental freedoms of EU citizens'[172] it is likely that its members will try to reconcile the Framework Decision with the spirit of the Directive and thereby develop a more coherent data protection scheme for the AFSJ. Furthermore, Europol and Eurojust are now part of the legal framework of the EU and the European Parliament has to give its consent whenever they are concluding agreements with third states.[173] Another important aspect that has to be mentioned with regard to the Lisbon Treaty is Article 16 of the Treaty on the Functioning of the European Union. This article is concerned with the protection of personal data and in addition to that, the 'European Parliament and the Council are obliged to provide data protection rules in all areas of EU law'.[174]

Article 16 TFEU:

> 1. Everyone has the right to the protection of personal data concerning them.
>
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

According to the last sentence of Article 16 TFEU, the compliance should be supervised by independent authorities. Here it is interesting to note that Article 8 of the Charter of Fundamental Rights of the European Union refers to exactly the same aspect by stating that the 'compliance with these rules shall be subject to control by an independent authority'.[175] Hence, data protection is regarded as a fundamental right of the European Union Article 8 should be valid for all the sectors and in accordance with that it should also be applicable to the supervision of external agreements in

[170] de Busser, 2010, p.90
[171] The Lisbon Treaty entered into force on 1st December 2009 and it amends the Treaty of Rome and the Treaty of Amsterdam. While the former was renamed to the Treaty on the European Union (TEU), the latter was renamed to Treaty on the Functioning of the European Union(TFEU). For more details see: Chalmers, Davies & Monti (2010). *European Union Law*. New York: Cambridge
[172] Nino, 2010, p.85
[173] Article 218 (6) (a) – (v) Treaty on the Functioning of the European Union
[174]For exact wording see: Hijmans (2010). *Recent Developments in data protection at European Union level* . ERA Forum, Vol.11, p.220
[175] Article 8 (3) of the Charter of Fundamental Rights of the European Union

security–related matters. Thus, it would be best to establish a new independent supervisory body which is responsible for monitoring the compliance with the data protection principles in security–related matters. This new supervisory authority should function in a similar way as the supervisory regime of Eurojust which has turned out to be very effective.

Furthermore, it is self-evident that it is 'much easier to control national actors than actors outside',[176] but in order to protect the fundamental rights of EU citizens to the largest possible extent, the 'adequacy principle' needs to be specified and better controlled. Due to the fact that 'the European system protects privacy stricter than the American one, the European Data Protection Supervisor recommends, for instance, to assess the data protection level before the actual start of the data exchange with the US'.[177] This risk assessment could also be executed by the newly introduced supervisory body. However, until today there is nothing like a European Public Prosecutor because this demands 'far–reaching inroads into the sovereignty of each state and further, the legal systems of the member states differ too widely'.[178] It is thus doubtful if and when the member states will effectively establish this independent supervisory body.

All in all, it can be said that data sharing is still considered to be necessary in order to deal with new forms of threats, like for instance terrorism. And for the conclusion of further data sharing agreements it is required that the AFSJ either modifies the existing Framework Decision or develops a new instrument which will be better in line with the fundamental data protection principles than the current Framework Decision. Eurojust can be used as a perfect example of how the modified and respectively new instrument as well as future cooperation and accordingly data sharing agreements with third countries should look like. If the European Union and its member states will in fact use Lisbon as the possibility for change, then they will be able to conclude data sharing agreements which are in balance between guaranteeing security and protecting fundamental rights of their citizens.

Bibliography

Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows (2001). European Treaty Series, No.108.

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record data by air carriers to the United States Department of Homeland Security (2007). OJ L 204, 04.08.2007.

Agreement between the European Union and the United States of America on the processing and transfer of passenger name records (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298, 27.10.2006.

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, Council of the European Union, 17434/11.

Agreement between the United States of America and Eurojust. 06.11.2006.

[176] For exact wording see: de Hert & de Schutter, 2008, p.302
[177] For exact wording see: Opinion of the European Data Protection Supervisor, 09.02.2012
[178] For exact wording see: Kapplinghaus, 2007, p.18

Andreas & Nadelmann (2006). *Policing the Globe: Criminalization and Crime Control in International Relations.* New York: Oxford University Press.

Archick (2011). *US - EU Cooperation against terrorism.* Congressional Research Service.

Bellanova (2009). Prüm: *A model 'Prêt - à - Exporter'? The 2008 German - US Agreement on Data Exchange*. Challenge Liberty and Security, No.13.

Bignami (2011). *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*. Boston College Law Review, Vol.48, pp. 609-698.

Birnhack (2008). *The EU Data Protection Directive: An Engine of a Global Regime*. Computer Law & Security Report.

Blas (2010). *Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom.* ERA Forum, Vol.11, pp. 233-250.

Blas (2009). First *Pillar and Third Pillar: Need for a Common Approach on Data Protection?* In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, & S. Nouwt, Reinventing Data Protection? Springer Science and Business Media, pp. 225-237.

Boehm (2012). *Data Protection Standards in the AFSJ. Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, pp. 19-173.

Brouwer (2011). *Ignoring Dissent and Legality: The EU's proposal to share personal information of all passengers*. CEPS Paper in Liberty and Security in Europe.

Chalmers, Davies & Monti (2010). *European Union Law*. New York: Cambridge.

Charter of Fundamental Rights of the European Union. (2000). OJ L 364, 18.12.2000.

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and 14, ETS No.5, 04.11.1950.

Convention for the protection of individuals with regard to automatic processing of personal data. (1981). European Treaty Series, No.108.

Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. (2002*).* OJ L 63, 06.03.2002.

Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20.05.2004.

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. (2009). OJ L 138, 04.06.2009.

Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information. (2009). OJ L 325, 11.02.2009.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008). OJ L 350, 30.12.2008.

Council of the European Union: Council adopts new EU–US agreement on PNR data, 9186/12, PRESSE 173, 26.04.2012.

de Busser (2010). *EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving its Citizens an American Meal*? Utrecht Law Review, Vol.6, No.1, pp. 86-100.

de Hert & Bellanova (2008). *Data Protection from a Transatlantic Perspective: The EU and US move towards an International Data Protection Agreement?* Brussels: European Parliament.

de Hert & Bellanova (2009). *Data protection in the Area of Freedom, Security and Justice: A system still to be fully developed?* Brussels: European Parliament.

de Hert & Bellanova (2011). *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals.* Washington, DC: Migration Policy Institute.

de Hert & de Schutter (2008). *International Transfer of Data in the Field of JHA: The Lessons of Europol, PNR and Swift. Justice, liberty, security: New challenges for EU external relations*, pp. 303-340.

de Hert & Papakonstantinouc (2009). *The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for*. Computer Law & Security Review, Vol. 25, pp. 403-414.

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement on such data. OJ L 281, 23.11.1995.

European Union (2009). *Treaty on the European Union.*Lisbon.

European Union Agency for Fundamental Rights (2011). *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.* Vienna.

Fletcher & Lööf (2008). *EU criminal law and justice.* Edward Elgar Publishing.

Geyer (2008). *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*. Challenge Liberty and Security, Vol.9, pp. 1-43.

Guild & Brouwer (2006). *The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US.* CEPS.

Hijmans (2010). *Recent Developments in data protection at European Union level*. ERA Forum, Vol.11, pp. 219-231.

Hijmans & Scirocco (2009). *Shortcomings in the EU data protection in the third pillar and second pillar. Can the Lisbon Treaty be expected to help?* Common Market Law Review, Vol.46, pp. 1485-1525.

Hix (2005). *The Political System of the European Union*. New York: Palgrace Macmillan.

Kapplinghaus (2007). *Eurojust: Signpost on the road to Security, Freedom and Justice in Europe*. Resource Material Series No.73, pp. 18-28.

Nino (2010). *The protection of personal data in the fight against terrorism: New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon*. Utrecht Law Review, Vol.6, No.1, pp. 62-85.

Nugent (2006). *The Government and Politics of the European Union*. New York: Palgrave Macmillan.

Opinion of the European Data Protection Supervisor, 09.02.2012.

Proposal from the European Commission *for Directive 96/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*: OJ No C 277, 05.11.1990 and OJ No C 311, 27.11.1992.

Punch (2006). *Developing Effective Research Proposals.* London: Sage.

Rules of procedure on the processing and protection of personal data at Eurojust 2005/C 68/01. (2005). OJ L 68, 19.03.2005.

Supplemental agreement between the European Police Office and the United States of America on the exchange of personal data and related information. 20.12.2001.

Tzanou (2010). *The EU as an emerging 'Surveillance Society': The function creep case study and challenges to privacy and data protection.* International Constitutional Law Journal, Vol. 4, pp. 407-427.