BACHELOR THESIS

Data Protection and Data Sharing in the Context of Transatlantic Counter-terrorism Cooperation

Case study of the EU-US SWIFT Agreement

Pia Sophie Hanbuch

s1855077

Student of the joint degree Public Governance across Borders

Westfälische Wilhelms Universität & University of Twente

First Supervisor: Dr. Claudio Matera

Second Supervisor: Dr. Pieter-Jan Klok

July 4, 2018

Abstract

Data-sharing agreements in the context of the transatlantic counter-terrorism cooperation have been attracting increased interest by academic scholars. This accounts for the fact that these agreements build the intersection of thematic areas surrounding the protection of personal data and the fight against terrorism both of which are of great interest in the wake of the digital age and an increasingly globalized world. Moreover, the legal framework with regards to the protection of personal data is constantly evolving and; therefore, makes it necessary to continuously study transatlantic data-sharing agreement and their consistency with existing law. This study aims to address this need by conducting a case study of the EU-US SWIFT Agreement which enables the transfer of personal financial messaging data from EU territory to the US for the purposes of fighting terrorism and its financing. Taking into account the different data protection standards within the EU and the US legal frameworks, as well as the consistency and applicability of the newly introduced EU secondary data protection legislation with the SWIFT Agreement, this study argues that the protection of EU citizen's personal data in the context of the EU-US SWIFT Agreement is not in accordance with EU data protection standards.

Keywords: 9/11, Counter-Terrorism, Data Protection, Data Transfer, Directive (EU) 2016/680, European Union, Fundamental rights, International Terrorism, SWIFT, TFTP, Unites States

List of Abbreviations

AFSJ	Area of freedom, security, and justice
CFREU	Charter of Fundamental Rights of the European Union
ECJ	Court of Justice of the European Union
The Commission	European Commission
Convention No. 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981
Data Retention Directive	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58EC
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECPA	The Electronic Communications Privacy Act of 1986
ECtHR	European Court of Human Rights
EP	European Parliament
EU	European Union
FBI	Federal Bureau of Investigation
FISA Act	The Foreign Intelligence Surveillance Act of 1978
Fourth Amendment	Fourth Amendment to the Constitution of the United States
GDPR	Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
JHA	Justice and Home Affairs
Judicial Redress Act	Judicial Redress Act of 2015
LE Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences

	or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/97/JHA
LIBE committee	Committee on Civil Liberties, Justice and Home Affairs
NSA	National Security Agency
NSL	National Security Letters
Privacy Act	Privacy Act of 1974
RQ	Main Research Question
SQ	Sub-question
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIFT(-II) Agreement	EU-US SWIFT Agreement
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program
Umbrella Agreement	Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses
US	United States of America
UST	U.S. Treasury Department
WP29	Article 29 Data Protection Working Party

Table of Content

1. Introduction:
Personal Data within a Digital and Globalised World

Data are the new oil. They encompass information which are being collected in almost every aspect of the daily life. Especially, business models such as Google, Facebook and co are based on users who constantly share personal information with them. Although the services of these internet giants do not seem to cost anything at first glance, users are paying with a very valuable asset: their personal data. Since personal data can inter alia provide the basis to track, manipulate or influence citizens, they are not only of great value for companies and their selective advertisement. Others have long recognized the benefits of the collected information, for example for well-directed election campaigns or criminal prosecution.

Problems arise when personal information is passed on and is further processed without the knowledge and consent of its owner. The sharing of data, however, has become easier in course of the digital revolution and data transfers have increased in speed and extent. Data is being processed and shared at all times by a wide range of agents, ranging from the previously mentioned tech-companies to ministries and law enforcement agencies, as well as airports or surgeries. The limitation to data access and data sharing of both companies and government agencies to protect privacy and to prevent misuses of personal data fall into the realm of politics and legislation.

Privacy and data protection are primary issues of concern for the European Union (EU) and the protection of personal data became a fundamental right with the entering into force of the Lisbon Treaty in 2009 (Hert & Papakonstantinou, 2018). Since the last legislative measure in the EU to protect personal data processing in the area of Justice and Home Affairs (JHA) was adopted in 1995 – a time in which future Facebook founder Mark Zuckerberg was only 11 years old – the European Union saw itself in the need to adjust EU data protection to the digital age. Therefore, a new data protection reform package was adopted on 27 April 2016. Within the reform package, ‘Regulation (EU) 2016/679’ (the GDPR) which regulates the general data processing of natural persons is accompanied by Directive (EU) 2016/680 (LE Directive) which regulates the “protection of natural persons with regard to the processing of personal data by competent authorities” for security purposes (European Parliament & Council, 2016a,b).

Personal data can be a valuable asset for law enforcement agencies as it can help to identify and track (alleged) perpetrators. Since the Treaty of Amsterdam entered into force in 1997, EU citizens are assured to live in an area of freedom, security, and justice (AFSJ)

(European Parliament/Think Tank. (n.d.)). “This implies the development of an effective fight against terrorism at the European level” (Dumitriu, n.d.), and the cooperation with third states – particularly the United States (US). The cooperation of the transatlantic partners consists inter alia of various data-sharing agreements. One of these agreements, the so-called EU-US SWIFT Agreement (SWIFT Agreement), will be the focus of this study.

The value of the access to personal data for counter-terrorism efforts coupled with the need to protect the EU fundamental right to the protection of personal data – especially in the context of the transfer of those data to third countries with other data protection jurisdictions – make the EU-US SWIFT Agreement an interesting object of investigation. This is particularly since the new LE Directive addresses the legal framework in the EU in which the SWIFT Agreement operates. This study will look at how the fundamental right to the protection of personal data of EU citizens is ensured by the SWIFT Agreement, considering the role of the EU within the power relationship of the transatlantic counter-terrorism cooperation and the new LE Directive.

1.1 Data Sharing within Transatlantic Counter-Terrorism Cooperation

The events of 9/11 constitute a turning point in the transatlantic counter-terrorism cooperation and have changed the perception of the threat of terrorism around the world (Rees, 2006). As a result, the terrorist attacks by the Islamic terrorist group Al-Qaeda on the World Trade Centre and the Pentagon led to the recognition of a new form of terrorism: ‘International terrorism’. International terrorism is the outcome of an increasingly globalized world with vanishing borders in time and space, enabling people and ideas to spread across the globe at an unprecedented scale. It is characterized by a cross-border nature, Islamic fundamentalism and a “more diffuse and non-hierarchical” array of largely independent extremists (Monar, 2015, p.336).

Shortly after 9/11, European member states held an extraordinary European Council meeting and concluded that “the fight against terrorism will, more than ever, be a priority of the European Union” (European Council, 2001, p.1). The EU not only acknowledges that terrorism is a main threat to its security but also that the transnational nature of terrorism demands cooperation between national actors within the EU and collaboration of the EU with international partners (Rees, 2006). In the extraordinary European Council meeting in 2001, the EU “calls for the broadest possible global coalition against terrorism” (European Council, 2001, p.1). Especially cooperation with the United States in law enforcement and intelligence have been “a top priority” of the European Union in its effort to combat terrorism (Archick,

2016, p.6). After all, US governments agree that the cross-border nature of terrorism makes it necessary to cooperate on multilateral levels. A close transatlantic counter-terrorism cooperation has been existing since the terrorist attacks of 9/11 and the importance of this cooperation was inter alia reaffirmed in an EU-US declaration to combat terrorism in 2004 in which the allies confirmed to "*remain determined to work together to combat terrorism while sharing a commitment to protect and respect human rights, fundamental freedoms and the rule of law on which our societies are founded and which terrorism seeks to destroy*" (European Council, 2004, p.1).

Nevertheless, the EU and the US counter-terrorism strategies that have evolved since 9/11 show several and sometimes fundamental differences. The European approach to counter terrorism has been influenced by several major terrorist attacks on European capitals[1]. Rik Coolsaet describes the EU Counter-terrorism Strategy as an event-driven counter-terrorism agenda and compares its development to "shock waves, propelled by major attacks, but gradually winding down once the sense of urgency had faded away" (Coolsaet, 2010, p.858). The reason for this is the fact that the protection of security is an issue that lies at the core of national sovereignty (Keohane, 2007). Therefore, harmonizing the cooperation of EU member states in the field of JHA has proven to be complicated because the EU is founded on the principle of conferral (Article 5(1) TEU) but EU member states do not easily hand over competencies to the Union level in this realm (European Union, 2012b; Archick, 2016). Two attacks on European capitals were crucial for the development of the European counter-terrorism strategy: Bombings on the Atocha metro station in Madrid in 2004 and in London in 2005. The latter contributed to the adoption of the first overall EU counter-terrorism strategy in 2005, mostly due to a proposal of the United Kingdom, which was holding the EU presidency at that time and wanted to bring "order to the chaos" (Coelsaet, 2010, p.860). Four strategic pillars: 'prevent', 'protect', 'pursue' and 'respond'[2] build the foundation of this strategy whereby the EU put the pillar 'prevent' at the front of the EU counter-terrorism strategy (Coolsaet, 2010). Subsequent investigations of the attacks in Madrid and London uncovered

[1] Madrid (2004), London (2005), Paris (2015), Brussels (2016), Nice (2016), Berlin (2016), Manchester (2017), London (2017), Barcelona (2017)

[2] 'Prevent' includes identifying and counteracting root causes and terrorist recruitment to preclude radicalization; 'protect' refers to the safeguarding from new attacks, 'pursue' means to "investigate terrorists and their networks" and 'respond' is intended to put into practice the 2004 solidarity clause by enhancing consequence management mechanisms and capabilities to be used in the event of an attack in one of the member states" (Coolsaet, 2010, p.861)

radical bases and cells within the EU from which the attacks were planned and "led to a transformation of (a) (…) primarily external to an at least partially also internal threat perception" (Monar, 2015, p.336). Within the European Union Security Strategy of 2003, the EU acknowledges that "Europe is both a target and a base for (…) (international) terrorism" (Council of the EU, 2009, p.31). This threat perception coupled with the location of counter-terrorism policies in the firmer third pillar before the adoption of the Lisbon Treaty in 2009 account for the fact that the EU counter-terrorism strategy focuses on the internal dimension of the terrorist threat and counter terrorism actions are located within the field of JHA. In sum, terrorism in the EU is treated as a crime which is to be dealt with by law enforcement and intelligence cooperation, and the EU counter-terrorism approach focuses on prevention and an internal dimension of the terrorist threat (Porter & Bendiek, 2012; Coolsaet, 2010).

In contrast, the counter-terrorism approach in the US in the aftermath of 9/11 put an emphasis on the external dimension of the threat and focused on fighting terrorism abroad (Keohane, 2007). US action to counter terrorism is still to a large extent militaristic and composed of interventions in the 'home-bases' of terrorism, mainly in the Middle East. According to Cian Murphy, one of the greatest differences between the counter-terrorism approaches of EU and US is the "idea of 'exception'", namely that the US is "putting in place a permanent emergency to allow extraordinary law enforcement and security powers to be extended" (Murphy, 2012, 230). However, the counter-terrorism approach of the US has been brought more into line with the EU counter-terrorism approach's focus in preventative measures (Porter and Bendiek, 2012). Furthermore, the EU and US strategies have in common that they see cooperation with third countries, in particular with the transatlantic ally, as one of the main pillars in the fight against international terrorism. This has led to the adoption of common several EU-US data-sharing agreements to deepen intelligence cooperation and to fight terrorist financing as well as easy border crossing of terrorists.

1.2 An Asymmetrical Relationship?

The power relationship within the transatlantic counter-terrorism relationship has been basis for a considerable amount of research. Porter and Bendiek (2012) find that the cooperation constitutes a "reciprocal (or, bidirectional) impact" leading to a convergence of EU and US counter-terrorism strategies and a shift of the US counter-terrorism approach towards the EU approach in its focus on prevention (Porter and Bendiek, 2012, p.497). Porter and Bendiek (2012) conclude that the SWIFT Agreement constitutes one example for norm convergence within the transatlantic counter-terrorism relationship and is "evidence the EU

has been able to maintain its firm commitment to robust privacy norms, all the while cooperating with the USA on important CT (counter-terrorism) programmes".

Els De Busser (2010) draws completely opposite conclusions on the cooperation of EU and US within the SWIFT Agreement and; thereby, represents the predominant opinion in current research on the power relationship within the transatlantic counter-terrorism cooperation. He concludes that EU-US agreements "continue along the same line of a lack of compliance with the basic EU level of data protection" (Busser, 2010, p.100). Also, Argomaniz (2008) concludes in a study on the Passenger Name Records Agreement (PNR Agreement) that "border security cooperation is far from being a 'partnership', resembling instead an asymmetrical relationship" (Argomaniz, 2008, p.120). Servent and MacKenzie (2012) take up Argomaniz's findings in their analysis on the SWIFT Agreement to answer whether the nature of the asymmetrical partnership changed in the aftermath of the Lisbon treaty which grants the European Parliament (EP) more rights in the ordinary legislative procedure. The EP has been identified by Argomaniz (2008) as the EU institution that is the greatest promoter of the right to the protection of personal data. Nevertheless, Servent & MacKenzie (2012) conclude that both EU and EP acted as norm takers of US security norms in the negotiations of the SWIFT Agreement despite the increased powers of the EP to co-decide on international agreements. Therefore, no supposed change of the EU's position within the power relationship in the transatlantic counter-terrorism cooperation took place (Servent & May Kenzie, 2012). In sum, the overwhelming amount of current research on the transatlantic counter-terrorism cooperation finds that the relationship is asymmetrically shaped towards the US. Furthermore, there is agreement about the fact that different data protection approaches in EU and US creates serious challenges for transatlantic counter-terrorism cooperation by means of data sharing agreements (Porter and Bendiek, 2012; Keohane, 2007; Archick, 2016).

1.3 Research Objective

In the following, the research objective of this study will be outlined and explained. As stated earlier, the focus of this research is the EU-US SWIFT Agreement. The SWIFT Agreement is part of the transatlantic counter-terrorism cooperation and enables the transfer of financial messaging data between the European Union and the United states. Therefore, the agreement is subject to the different data protection approaches of EU and US that have been found to challenge the transatlantic counter-terrorism cooperation in previous studies. However, the different approaches to data protection not only challenge the transatlantic counter-terrorism cooperation but might also have an effect on the extent to which transferred data are

protected within the SWIFT Agreement. It is the objective of this research to analyse the protection of the EU fundamental right to the protection of personal data within the SWIFT Agreement by answering one the main research question (RQ):

To what extent does the EU-US SWIFT-Agreement protect personal data of EU citizens in accordance with relevant EU data protection legislation and standards?

The core of the analysis will be a case study on the EU-US SWIFT Agreement. In order to draw conclusions on the extent to which the SWIFT Agreement protects the personal data of EU citizens, both the EU and the US legal data protection frameworks will be analysed. Based on existing literature it is assumed that the data protection frameworks differ in terms of their data protection standards. Therefore, the data protection standards of the EU and the US legal framework will be compared.

Within the case study, the role of the EU in the negotiation process of the SWIFT-Agreement will be taken into account to examine whether the EU managed to integrate EU data protection standards in the agreement. Thereby, the power relationship within the transatlantic counter-terrorism cooperation will be considered. The main objective of the case study is to analyse whether the data protection provisions within the SWIFT Agreement are in accordance with the data protection standards of the EU data protection framework. According to Article 7 TFEU, the European Union has the duty to "*ensure consistency between its policies and activities*" (European Union, 2012c). Furthermore, Article 21 TEU requires that the European Union's "*action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement*" (European Union, 2012b), which includes the respect for human rights and fundamental freedoms. Since the right to the protection of personal data is included within the treaties of the EU as a fundamental right, the European Union is required to act in guidance with this right when adopting international agreements such as the SWIFT Agreement. The data protection provisions within the SWIFT Agreement can be said to be in accordance with the EU data protection standards when they are consistent with the policies and fundamental law provisions of the EU treaties.

This study, furthermore, aims to include the newly introduced LE Directive which, like the SWIFT Agreement, must be in accordance with EU data protection standards within the EU treaties. The purpose is to analyse the consistency of the SWIFT Agreement and the LE Directive. Thereby it will be seen, whether the EU ensures in its data protection framework for consistency of its policies. The study furthermore aims to examine whether the supposed

increase in EU data protection as result of the LE Directive changes the position of the EU within the EU-US power relationship. Throughout the analysis it will be seen whether the data protection provisions within the SWIFT Agreement have been and continue to be in accordance with applicable data protection law within the EU.

1.4 Societal and Scientific Relevance

Since the EU-U.S. SWIFT agreement builds an important component of the EU counter-terrorism strategy and encompasses the transfer of financial messaging data from the EU to the US it plays an important role in the legal realms of both data protection and security (counter-terrorism). Both the protection of personal data and the protection of security are enshrined as rights within European treaties. Within the preamble of the Charter of Fundamental Rights of the European Union (CFREU), the EU commits itself to put "the individual at the heart of its activities, by establishing the citizenship of the Union and by creating an area of freedom, security and justice" (European Union, 2012a). The right to liberty and security of the person is furthermore assured for in Article 6 CFREU, directly followed by the rights to privacy and data protection in Articles 7 and 8 CFREU. Furthermore, both the fight against terrorism and the protection of personal data are of great importance to European society.

Terrorism got international momentum after the events of 9/11 and has gained importance in the EU in the aftermath of a series of terrorist attacks in European capitals since 2004. Especially recent terrorist attacks in France, Belgium and Great Britain in combination with the European migration crisis make international terrorism an issue that lies at the heart of European citizens' minds. In a Eurobarometer survey of 2016, 87% of European citizens consider terrorism a high or medium risk (European Parliament, 2016). Also, the protection of personal data has become increasingly important to European society because digitalization affects nearly every aspect of everyday life. Concerns of European citizens regarding their personal data have been identified in a Eurobarometer study of 2015 which "demonstrates that Europeans have widespread concerns about the consequences of their data being misused" (European Commission, 2015a). 'Misuse' occurs, by definition, in "an occasion when something is used in an unsuitable way or in a way that was not intended" (Cambridge Dictionary, 2018). Misuse therefore also occurs when data which have been acquired for commercial or financial purposes are further used and processed by police or justice authorities for security purposes.

Although the use of data for security purposes may be essential to ensure security, personal data must be protected against disproportionate utilization by governments or public authorities. After all, it is not only the protection of security that is enshrined in law and that is important to the people of the EU, but also the protection of personal data. Since the SWIFT agreement plays an important role in the legal realms of both data protection and security it is important that the concerns of EU citizens and the rights of EU citizens are taken into account by the agreement. In that sense it is furthermore of great importance to study how the EU - within the negotiations of the SWIFT agreement and by enacting new data protection legislation - manages to protect EU citizens security on the one hand while not undermining the right to the protection of personal data in the SWIFT agreement on the other. While Porter and Bendiek (2012) found that the role of the EU as a norm taker within the transatlantic security cooperation did not change in the aftermath of the Lisbon Treaty, it is of interest to analyse whether the LE Directive manages to change the role of the European Union in the transatlantic counter-terrorism relationship.

Furthermore, the fact that most current research on the SWIFT agreement is based on a legal framework which has been amended by the LE Directive increases the need to study the compatibility of the agreement with the LE Directive. Despite the pressing concerns of European citizens regarding their privacy and security only limited attention is given to the LE Directive which addressed both these issues. While the GDPR and data sharing agreements in the commercial realm, for example the Privacy-Shield agreement, are recurrently analysed and are paid a lot of attention in the media, data sharing agreements within the realm of EU justice and home affairs are granted much less attention.

2. Methodology and Research Design

In order to answer the RQ, three sub-questions (SQs) have been identified and will be presented within the following chapter (2.1). This is followed by an explanation of concepts and legal principles which will be of relevance for the subsequent analyses (2.2). US legislation, EU primary and secondary legislation and the EU-US SWIFT Agreement, as well as existing relevant literature are the basis of this research. The different policies and legal measures of the EU and the US data protection frameworks, the SWIFT agreement and the LE Directive will be described, explained and analysed in depth in the subsequent chapters 3 to 5.

2.1 Sub Questions

The sub-questions represent approaches to a combination of evaluative, empirical, explanatory and hermeneutic types of research (Matera, 2016). Together, the answers to these SQs in chapters 3 to 5 will lead to answering the RQ in chapter 6.

1) What are the differences of the EU and the US approach to data protection? (Chapter 3)

Sub question one follows an empirical-explanatory-hermeneutic type of research and will be answered using a comparative approach (Matera, 2016). Chapter 3 will start with an analysis of the differences in EU and US privacy perceptions which are the basis for the differences in EU and US data protection frameworks. Focus of chapter 3 will be the different data protection frameworks of the EU and the US. First, the EU data protection principles will be identified and explained (3.1). Hereby, the focus will be on EU primary law which establishes EU standards for the protection of privacy and personal data and which builds the foundation for EU secondary legislation. Additionally, the European Council Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data will be considered. The council convention builds an overall framework for EU data protection because all EU member states are party to the convention. The analysis of the EU legal data protection framework is followed by the analysis of the US data protection framework (3.2). After extensive identification and explanation of both the EU and the US data protection standards, the two data protection regimes will be compared regarding their compatibility to answer SQ1 (3.3). Therefore, the answer to SQ1 will also include a systemic approach because the consistency and coherence of EU data protection standards with U.S. data protection standards will be part of the comparative analysis (Matera, 2016).

2) Is the level of data protection within the SWIFT Agreement consistent with the data protection principles of the EU treaties? (Chapter 4)

Sub Question two takes the approach of an explanatory and evaluative type of research and will be answered within chapter 4 of this study. SQ2 comprises the case study of the SWIFT Agreement. Chapter 4 will begin with a historical review the Agreement, taking into account the development of the US Terrorist Finance Tracking Program and the negotiation procedure of the SWIFT agreement (4.1). Then, the data protection provisions of the SWIFT Agreement will be analysed regarding their accordance with the EU data protection principles that have been identified within chapter 3.1 (4.2). This is followed by conclusions and the answer to SQ2 within chapter 4.3. Throughout the whole analysis of the SWIFT Agreement, the power relationship of EU and US will be considered.

3) To what extent is the level of data protection within the SWIFT agreement consistent with the newly introduced Law Enforcement Directive? (Chapter 5)

Sub Question three takes an explanatory and hermeneutic approach (Matera, 2016). Chapter 5 will focus on the content of the LE Directive and the compatibility of the data protection provisions within the SWIFT agreement with the content of the LE Directive. To answer this sub-question, a systemic approach will be used (Matera, 2016). The LE Directive will be analysed regarding the scope of its applicability (5.1) and its data protection right and principles (5.2). Hereby, especially the data protection provisions concerning international agreements and data transfers to third states will be considered (5.3). In the conclusion of chapter 5 it will be answered whether the data protection provisions of SWIFT Agreement and LE Directive are compatible (5.4)

2.2 Concepts and General Legal Principles

2.2.1 Privacy and Personal Data

The definition of what the term "private" means is part of a fundamental debate which has not yet produced a general definition. Daniel J. Solove (2002) provides a comprehensive account of existing conceptualizations of privacy which he summarizes in six categories: "the right to be left alone", "protection of personhood", "intimacy", "limited access to the self", "secrecy" and "control over personal information". For the purpose of this research, the last three categories are of particular relevance due to their focus on personal information. In this vein, privacy is defined as "concealment of information", "the individual's ability to ensure that personal information is used for the purposes she desires" or "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Solove, 2002, 1105-1110). Also, Alan Westin (2003) has defined privacy in terms of personal information, namely as "the claim of an individual to determine what information about him or herself should become known by others" (Westin, 1967, p.1). Therefore, the concepts of privacy and personal data are closely related. Since this study will analyse the extent to which the SWIFT Agreement protects personal data in accordance with relevant EU standards, it is necessary to understand what the EU perceives as personal data. The Court of Justice of the EU (ECJ) has, in several judgments relating to the protection of personal data, included a range of information under the category of personal data, for example name, telephone number, hobbies or fingerprints (Laudati, 2016, p.38). Overall, personal data is defined in the EU as "any information that relates to an identified or identifiable

living individual" (European Commission, 2018b). The connection of the right to privacy and the right to the protection of personal data can also be perceived within the EU legal framework on data protection which will be analysed in the following chapter.

2.2.2 Lex Posterior, Lex Specialis, Lex Superior

The research is conducted from a legal perspective and is therefore following an empirical, qualitative and conceptual approach based on several principles of legal research (Matera, 2016). The principles which are of importance regarding the analysis of the EU data protection legal framework are Lex Posterior, Lex Specialis Derogat Generali and Lex Superior Derogat Inferiori. These principles are used in case of a norm collision to decide which law applies and the meaning and application of these principles can be explained by their translation from Latin into English.

The principle Lex Specialis Derogat Legi Generali implies that the general law (lex generalis) is subsidiary to the special law (lex speciallis) (Rechtslexikon.net., n.d.a). The principle Lex Superior Derogat Legi Inferiori implies that the norm that is higher within the norm hierarchy breaks the lower law. Within the European Union, EU treaties (EU primary law) are at a higher position within the norm hierarchy than International agreements or EU secondary law (Rechtslexikon.net., n.d.b). The principle Lex Posterior Derogat Legi Priori implies that a law that is enacted later in time trumps the older law (Rechtslexikon.net, n.d.c).

2.2.3 Data Protection Rights and Principles

The important data protection principles and provisions that have been found and that are of importance for the aim of this study have been classified within four overall categories: Lawful processing, transparency, control and review mechanisms, effective remedies. Based on these categories it will be analysed whether the data protection provisions of the SWIFT Agreement are consistent with EU primary law and with the LE Directive. Since these four categories will serve as a guideline to analyse the consistency of the SWIFT Agreement with the EU data protection framework, the core principles and the rights they include will shortly be introduced in this section to allow for a structured analysis to answering of the RQ. However, an extensive analysis and explanation of these principles and rights will be given in chapter 3, 4.2.2 and 5.2. of this analysis.

Lawful Processing	- Processing in accordance with the law and on a legitimate basis - Purpose limitation principle (including the principle of necessity) - Data quality principles (relevance, accuracy, limited data-retention) - Accountability and Safety
Transparency	- Right to know (If and for what purposes personal data is being processed) - Right to access - Right to rectification, erasure, blocking
Control and Review Mechanisms	- Independent supervision/monitoring of processing - Review of implementation
Effective Remedies	- Right to be informed about possibility to seek redress - Right to seek redress - Right to compensation

3. EU and US Data Protection Frameworks: Dignity and Proportionality vs Liberty and Reasonableness

The right to privacy is protected in Article 12 of the Universal Declaration of Human Rights:

> "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*"
> (UN General Assembly, 1948).

Therefore, the right to privacy is a universal right. In order for privacy to be adequately protected within a globalised world, the details and scope of this right need to be understood in the same way across countries because personal data travels across borders and jurisdictions. However, different privacy and data protection frameworks evolved in the EU and the US and can hamper the equal protection of privacy. This could, in turn, lead to an inconsistent protection of personal data in the EU-US SWIFT Agreement which comprises the transfer of personal data from EU jurisdiction to US jurisdiction. This chapter is intended to examine the different data protection standards of the EU and the US legal data protection frameworks.

To understand the differing data protection frameworks, one needs to consider the different perceptions of privacy which prevail within European and American societies. James Q. Whitman (2003) tried to unfold the different perceptions that are deeply anchored in peoples' minds and is of the opinion that "we must acknowledge (…) that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly laws of privacy" (Whitman, 2003, p.1160). He refers to the conceptions of privacy which have been distinguished by Robert Post and which display the contrast of "privacy as an aspect of dignity and privacy as an aspect of liberty" (Whitman, 2003, p.1160). According to Whitman, "continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity" while privacy in America is much more related to liberty against the state, and the protection of privacy concerns mostly regard the sanctity of the home (Whitman, 2003, p. 1161). These different privacy perspectives are mirrored to a large extent in the data protection frameworks of EU and US which are analysed in this chapter. After the data protection frameworks haven been analysed, a connection will be drawn to the European and American privacy perception.

In the EU, there is different data protection legislation at the EU level, the EU member state level and at the level of different policy areas. The legal data protection system of the EU is characterized by the principle of subsidiarity. Thus, the EU competences are limited to the areas in which the EU member states have handed over their competences to the EU bodies. Counter-terrorism actions are located within the area of Justice and Home affairs and law enforcement. Here, the EU member states still play a major role because security has always been a policy area which is at the heart of national sovereignty. Therefore, the EU takes the role of a supportive body and aims to harmonize legislation of EU member states in this area by enacting Directives, Regulations and Action Plans regarding data sharing within the EU and with third countries. Despite the member state dominance, the EU is nevertheless becoming an important actor in the areas of counter-terrorism and privacy protection. EU legislation in these

realms is of great importance as both counter-terrorism and data protection need an overall legal framework to work effectively and, for example, to share data between countries and agencies to find terrorists who can travel freely past open borders in the EU. Therefore, the focus of this study will be the European Union policy level while excluding different national laws which would exceed the scope of this study. Furthermore, the analysis of the EU data protection legal framework will be focused on the area of law enforcement and counter-terrorism actions of the EU.

As the analysis will demonstrate, some of the EU data protection rights can be discovered in US Acts, however, with extensive restrictions concerning their applicability for non-US persons[3]. The legal data protection framework of the United States consists of measures at both the federal level and the state and local levels. The scope of the study is limited to the federal level of the US and on sectoral laws including data protection measures in the realms of national security and law enforcement since these are of most relevance for the analysis of the SWIFT Agreement. Despite the fact that there are several bilateral agreements between single EU member states and the US, the European Union policy level and the US federal level are of importance for the later analysis of bilateral data sharing agreements enacted between the EU and the US.

3.1 EU Data Protection Framework

The Council of Europe claims that its 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981' (Convention No. 108) "is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data" (Council of Europe, n.d.). Since all EU member states are party to Convention No. 108, it constitutes the basis for data protection regulations within the European Union, and its data protection guarantees can be found in both the European Convention on Human Rights and Fundamental Freedoms (ECHR) and the EU treaties. Due to the principles lex speciales, lex superior and lex posterior, however, the latter two are the most important legal sources regarding the protection of privacy and personal data

[3] In accordance with the study of Prof. Dr. Franziska Boehm for the Committee on Civil Liberties, Justice and Home Affairs (LIBE committee), this analysis will use the term "US persons" when speaking of people who are either US citizens or are permanent residents in the US. (Boehm, 2015)

within the EU and will therefore be the focus of the analysis of the EU data protection legal framework.

The Charter of Fundamental Rights of the European Union (CFREU), the Treaty on the Functioning of the European Union (TFEU) and the Treaty of the European Union (TEU) represent the primary law in the European Union. Since the Treaty of Lisbon entered into force in 2009, the right to the protection of personal data is specifically protected within Article 16 TFEU: *"Everyone has the right to the protection of personal data concerning them*" (European Union, 2012c; Hert & Papakonstantinou, 2018).

Before discussing EU primary law provisions on data protection, one must consider Article 8 ECHR and the respective case law of the European Court of Human Rights (ECtHR). While the European Court of Justice of the EU (ECJ) did not have any competence in law enforcement related matters on data protection prior the entering into force of the Lisbon Treaty, the ECtHR established important principles, which are now also applied by the ECJ (Boehm, 2015). Article 8 ECHR is also of particular importance to the EU data protection framework because Article 6(2), (3) TEU lays down that *"(t)he Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms (…) and Fundamental rights, as guaranteed by the (ECHR) (…) shall constitute general principles of the Union's law*" (European Union, 2012b). Article 8 ECHR reads as follows:

> *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.*
> (Council of Europe, 2010)

The ECtHR repeatedly interpreted Article 8(1) ECHR in accordance with Convention No. 108, finding personal data to be an important component of the right to private and family life. Furthermore, by referring to "everyone" in paragraph one, Article 8 ECHR does not exclude citizens of states that are not party to the convention from the scope of its applicability. Nevertheless, the Article is not free from limitations. Article 8(2) ECHR lays down possible exceptions, the most important ones in the context of this study being exceptions for the

purposes to protect national security and public safety. Based on Article 8(2) ECHR, the ECtHR established a three-step test in its case law to adjudicate on possible interferences and violations with the rights to privacy (Article 29 Data Protection Working Party, 2014a). After determining an interference with Art. 8(1) ECHR, this test includes an examination according to Article 8(2) ECHR of whether or not the interference is in accordance with the law, has a legitimate aim and is necessary in a democratic society. The Article 29 Data Protection Working Party (WP29) further defines the content of the test. Thus, criteria one is fulfilled if there is a legal basis for the interference and if the "activity (…) provides clearly defined rules governing how the activity will operate", which "clearly set out the extent of any discretion given to the law enforcement authority and guidance how that discretion should be exercised and provide adequate legal safeguards" (Article 29 Data Protection Working Party, 2014a, p. 6). A legitimate aim is given when the interfering activity is executed "in the interests of national security, public safety" or one of the other provisions laid down in Article 8(2) ECHR. The ECtHR usually focuses on the last step where it examines the proportionality of the balance between the necessity for democratic society and the protection of personal data (Boehm, 2015). Here, the ECtHR developed the general fundamental rights concepts of proportionality and necessity and thereby set the foundation for the application of these concepts in the realms of privacy and data protection in connection with law enforcement and intelligence. According to this, an action is necessary in a democratic society when it addresses a pressing social need, is proportional as well as relevant and sufficient. While the first and last requirements are to a large extent self-explanatory, the second requirement is further divided into five components. To be proportional, the action needs to "set clear aims and be purpose specific", follow the consideration of existing measures and alternatives, "ensure adequacy and relevance without excessiveness", set the data retention period and apply a holistic approach" (Article 29 Data Protection Working Party, 2014a, p.20-22). The concepts of proportionality and necessity occur in every EU treaty and secondary law measure that regulate data protection and privacy with regard to law enforcement and intelligence.

The treaties of the EU delineate the norms, values and standards on which the community is build and thus build the foundation for the protection of privacy and personal data. The rights to the protection of privacy and data protection are codified within Articles 7 and 8 CFREU as well as Article 16 TFEU. While Article 7 CFREU mirrors Article 8(1) ECHR, Article 8 CFREU and Article 16 TFEU specifically encompass the protection of personal data. Article 8 CFREU reads as follows:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3. Compliance with these rules shall be subject to control by an independent authority.*
> (European Union, 2012a)

The fact that one article within the CFREU is specifically dedicated to the protection of personal data distinguishes it from the ECHR and underlines the importance that the EU grants to the protection of personal data in treating it as a fundamental right. While Article 16(1) TFEU is identical with Article 8(1) CFREU, paragraphs (2) and (3) of the same article lay down the procedural provisions of data protection within the European Union:

> "*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*".

From these treaties and case law on these treaties derive the principles for data protection, as well as the structural provisions for legislation on data protection within the European Union, both of which are further codified in EU secondary law. The most important guarantees which are entailed in secondary law and specifically mentioned in Article 8 CFREU and Article 16 TFEU have been summarized within a study for the Committee on Civil Liberties, Justice and Home Affairs (the LIBE committee) and are purpose limitation, fair processing on basis of consent or another legitimate legal basis, the rights of access and rectification, and the right to independent oversight (Boehm, 2015). The purpose limitation principle "intends to considerably limit the use of collected data" (Boehm, 2015, p.14). The guarantee of fair processing presupposes that any data collection authority needs to stick to a transparent procedure, including the notification of the data subject of the data collection. This principle is the "pre-condition for invoking other rights, such as access, objections or rectification" (Boehm, 2015, p.14). Furthermore, it is required that data can only be collected

in the consent of the data subject, unless there is another legitimate legal basis as codified within secondary EU law. In case of another legitimate basis besides the consent of the data subject, "data processing (…) needs to be necessary, meaning that a balance between the different interests at stake needs to be met in each individual case" (Boehm, 2015, p.15).

The principle of necessity is also included within provisions for possible limitations of the fundamental rights within Articles 51, 52 and 53 CFREU. These mirror and add to the exemptions that are entailed within Article 8(2) ECHR. Article 51 specifically links any limitation of the fundamental rights to the principle of proportionality. Similar to Article 8 ECHR, Article 52 CFREU requires limitations to be necessary and to "*meet objectives of general interest (…) or the need to protect the rights and freedoms of others*". Furthermore, limitations need to be "*provided for by law and respect the essence of those rights and freedoms*" (European Union, 2012a). The ECJ has competence to decide on data protection matters within the realm of law enforcement since the previous pillar structure was dissolved by the Lisbon treaty. Like the ECtHR, the ECJ also focuses on the principle of necessity and proportionality when looking at limitations and possible interference or violation with data protection principles within the fundamental rights of the EU (Boehm, 2015). Since EU secondary law and international agreements need to be consistent with EU primary law, they are also subject to the concepts of proportionality and necessity. Article 16 (2), (3) TFEU furthermore provides that the rules relating to data protection must be laid down using the ordinary legislative procedure. This includes the European Parliament which had been excluded from the legislative procedures prior to the Lisbon Treaty.

These new powers that the Lisbon Treaty grants the EP which has always been a promoter of the protection of privacy rights in the EU and the rising awareness of the need to align data protection standards to technological and global developments have contributed to the adoption of a new data protection reform package on 27 April 2016 (Hert & Papakonstantinou, 2018; Reding, 2018). The reform package includes 'Regulation (EU) 2016/679' (the GDPR) and 'Directive (EU) 2016/680' (LE Directive). The former regulates the "processing by an individual, a company or an organisation of personal data relating to individuals in the EU" (European Commission n.d.). The Law Enforcement Directive codifies the rules on the "protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data" (European Parliament & Council, 2016a). Both the GDPR and the LE Directive confirm the universal nature that the EU assigns to the fundamental right to personal

data in that it states that "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data" (European Parliament and Council of the EU, 2016a,b).

Summarized, data protection and privacy are fundamental rights in the European Union and are therefore of high importance within the legal system of the EU. They are enshrined in the primary law of the EU which constitutes the basis on which the EU is build and can therefore be considered "constitutional provisions". The treaties "entail (…) important substantive data protection guarantees, which are, however, only a starting point for a much more elaborated data protection system developed in secondary law" (Boehm, 2015, p.16). The GDPR and the Law Enforcement Directive lay down the rules governing the rights. Both primary and secondary law of the EU ensure that the right to the protection of privacy and personal data within the European Union is granted to every natural person. This fact in combination with the primary law guarantees and detailed data protection principles, procedural requirements and possibility to remedies within EU secondary law constitute a comprehensive data protection framework, ensuring that personal data of individuals are sufficiently protected.

3.2 US Data Protection Framework

As will be seen throughout this analysis, data protection in the US is much more limited than within the EU. The US data protection legal framework is characterized by exceptions to data protection guarantees rather than comprehensive data protection measures. First, this accounts for the fact that there is significantly less constitutional protection of privacy and personal data within the United States when compared to the EU. The Fourth Amendment to the constitution holds that

> *"(t)he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*
> *(U.S. Const.)*

This is understood to include the protection of personal data and the examination of such data must therefore be "reasonable". However, the Fourth Amendment has two major

limitations regarding the protection of personal data in the context of the SWIFT Agreement. First, it is limited to US citizens and permanent residents in the US ("the people") and therefore does not apply to EU citizens. Second, searches and seizures in the context of personal data have only been understood to be "unreasonable" in cases in which an individual has a "legitimate expectation of privacy" (Bignami, 2015, p.10). In the past, this has led to the establishment of the so called "third Party Doctrine" which excludes personal data from the scope of the Fourth Amendment when it has been handed over voluntarily by the individual to a third party (Bignami, 2015, p.10). Therefore, most data which is collected by, for example, social media sites, financial institutions or other commercial companies is excluded from the scope of the Fourth Amendment.

Next to the Fourth Amendment, the Privacy Act of 1974 is the second source that aims for a comprehensive protection of personal data in the US and to "*balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them*" (U.S. Department of Justice et al., 2013). The Act follows four overall goals: Restricting disclosure of personal information, granting individuals "increased rights of access to agency records maintained on them" as well as the "right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete", and to "establish a code of 'fair information practices' which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records" (U.S. Department of Justice et al., 2013). The Privacy Act is the most comparable US data protection measure to EU data protection standards and principles. Analogical, it includes regulations on the transparency of personal data processing, on the "accuracy, relevance, timeliness, and completeness" of the processed personal data and on the kind of information a governmental agency is allowed to retain. The latter provision is very similar to the EU principle of proportionality as it requires that data collection is limited to "such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President" (Bignami, 2015, p.11). The one to whom the personal data pertains has furthermore the right to demand the correction of incorrect, irrelevant, outdated and incomplete data and data sharing requires the consent of this individual. Also, legal oversight is granted and individuals whose privacy rights have been violated have the right to sue the government (Bignami, 2015).

Nevertheless, the scope of the Privacy Act is much more confined than EU data protection measures and its applicability is limited by several serious exceptions: There are no regulations on data retention periods and, similar to the Fourth Amendment, the Privacy Act does not apply to foreigners and therefore not to EU citizens. Moreover, applicability is limited to "systems of records" thus excluding any data not included in a system from which government agencies retrieve information including "personal identifies"[4](Bignami, 2015). Also, the regulation of data sharing is subject to limitations. "'Routine uses' that are disclosed to the public at the time the record system is created, and (sharing) for a civil or criminal law enforcement activity" are exempt from the provision (Bignami, 2015, p.11). The study of the LIBE committee highlights the fact that oversight of the data collection and processing in the realm of law enforcement is the duty of the Privacy Office in the Department of Homeland Security and the Department of Justice, thus not comparable with the independent oversight bodies within the European Union and that, due to various general and specific exemptions, the law enforcement agencies are almost completely exempt from the obligation to comply with the duties of the Privacy Act (Bignami, 2015).

The Judicial Redress Act of 2015 (Judicial Redress Act) aims to improve the applicability of the Privacy Act to foreigners and establishes that three out of the four remedies of the Privacy Act are available to most EU citizens since they belong to the category of so called "covered countries" (Boehm, 2015). Denmark, Ireland, and the United Kingdom are, however, excluded from the scope of the Judicial Redress Act and are only treated as "covered countries" when they notify the US that they decided that the Data Protection and Privacy Agreement (DPPA, or the "Umbrella Agreement") applies to them (Judicial Redress Act of 2015, n.d.). This "Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses" (Umbrella Agreement) has been adopted in 2015.

> "*The purpose of this Agreement is to ensure a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism*."

[4] "Personal Identifiers" can be, for example, name, social security number or fingerprints (Bignami, 2015, p.11).

(European Union and United States of America, 2015)

According to the European Commission, the agreement "puts in place a comprehensive high-level data protection framework for EU-US law enforcement cooperation" and will improve the data protection of EU citizens in the transatlantic relations. Comparable to data protection measures in the EU and the Privacy Act, the Umbrella Agreement includes provisions on purpose limitations, time, access and rectification, data sharing, transparency and on remedies (European Commission, 2015b).

What is crucial regarding this study is the fact that law enforcement and intelligence agencies in the US have various means to access data. These ways of data collection are legally codified within several sector specific US Acts, for example, the Foreign Intelligence Surveillance Act (FISA Act), the USA Patriot Act and the Electronic Communications Privacy Act (ECPA). As these Acts also encompass data protection provisions to some extent, they are also of importance when discussing the legal data protection framework of the United States. Within her study for the LIBE committee, F. Bignami (2015) lists six different means that law enforcement agencies can use to collect personal data, three of which are used in the realm of ordinary criminal investigations (Bignami, 2015, p.15-19). Most of these measures focus on the collection of communication (meta)data within the Electronic Communications Privacy Act (ECPA)[5] and are only of minor importance to this study. Nevertheless, two aspects should be noted. First, EU and US nationals share the same data protection rights in the realm of ordinary criminal investigations, although US rights are of an overall lower standard when compared to EU data protection principles. Second, administrative subpoenas played a crucial role within the Terrorist Finance Tracking Program (TFTP) of the US and are therefore of importance regarding the analysis of the EU-US SWIFT agreement in chapter four of this study. In the period after the 9/11 attacks, US agencies made use of administrative subpoenas to get access to financial data of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Administrative subpoenas are paradigmatic for the low data protection standards within the US: The courts found data collection to be reasonable as long as the investigation was conducted pursuant to a legitimate purpose and was relevant for this purpose. In case of the TFTP, this purpose was "the mandate, set down by Congressional law

5 „The Electronic Communications Privacy Act ECPA is the main federal statute that regulates electronic surveillance in connection with investigating ordinary crimes. It is comprised of three acts: (1) the Wiretap Act; (2) the Stored Communications Act; and (3) the Pen Register Act" (Bignami, 2015, p. 17).

and Presidential executive order, to block 'the property of, and prohibited transactions with, persons who commit, threaten to commit, or support terrorism.'" (Bignami, 2015, p.17). Neither the Privacy Act nor the Fourth Amendment set any regulations on this data collection because the former permits data sharing for law enforcement purposes, and provisions of the latter did not apply because of the "third party doctrine".

In the realm of national security, data protection measures are included within the regulation of national security letters (NSL), the Foreign Intelligence Surveillance Act (FISA), the USA PATRIOT Act, and Executive Order 12,333. Within all these means and legal instruments there is a significant breach between data protection safeguards of US persons and foreigners, including EU nationals, since they aim to "ensure that US persons will be minimally implicated by foreign intelligence surveillance or at least not burdened in the exercise of their speech and association rights" (Bignami, 2015, 20).

National Security Letters (NSL) are the administrative subpoenas of national security investigations. They can be used by the Federal Bureau of Investigation (FBI) to get access to personal data which has been collected within ordinary criminal investigations under the Stored Communications Act, the Right to Financial Privacy and the Fair Credit Reporting Act. In this way, the FBI can obtain personal data from financial institutions and consumer reporting agencies. The legal requirement for the data collection is "that the information requested is 'relevant to an authorized investigation to protect against terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States'" (Bignami, 2015, p.21).

Beside NSLs, Section 702 of the FISA Amendment Act and Executive Order 12,333 authorize far-reaching surveillance of foreign intelligence information[6], including accessing of communications, content, metadata or other records by governmental agencies. The Foreign Intelligence Surveillance Act (FISA) originally covered "electronic surveillance" and "metadata surveillance". The USA PATRIOT Act expanded the scope of FISA to include "any tangible things" which includes non-content data of books, records, papers, or documents. The FISA Act prescribes the adoption of "minimization procedures" to limit the collection,

[6] Foreign intelligence is defined within the FISA Act as intelligence "that includes information that serves to protect national security against foreign threats (including international terrorism) and information that affirmatively advances the foreign affairs and national defence interests of the United States" (Bignami, 2015, p.22)

retention and sharing of information in several data collection measures and furthermore includes the FISA court as a review mechanism. However, there are obvious quality differences in data protection safeguards for US persons in comparison to foreign citizens. In traditional FISA orders, for example, only US persons have the possibility to file a suit for damages if they have undergone unlawful surveillance, and foreign citizens are excluded from the minimization procedure in the data collection of "any tangible things". Furthermore, the existing data protection safeguards are subject to wide-ranging exemptions if the data is collected for law enforcement purposes (Bignami, 2015). The already extensive FISA surveillance was even further expanded with Section 702 of the FISA Amendment in 2008 The government now "may collect foreign intelligence information of any type (…), on any person reasonable believed to be a non-US person overseas without making any of the specific showings required for electronic surveillance, metadata surveillance or tangible things" (Bignami, 2015, 25). Section 702 has been used to legitimize the PRISM and the NSA programmes.

Executive Order 12,333 regulates foreign surveillance which is not covered by the FISA Act and coincides with the FISA Act's double track regarding data protection standards for US citizens and foreign citizens. Thus, the departmental guidelines which set collection, retainment and dissemination procedures, as well as the requirement of approval by the Attorney General for data collection does not apply to foreign citizens and residents outside the United States.

Several reforms have been adopted since the revelations of Snowden in 2013, the two most important ones being the already described Judicial Redress Act, as well as Presidential Policy Directive-28 in 2014 and the FREEDOM Act in 2015. Presidential Policy Directive -28 aims to decrease the differences in data protection between US persons and non-US persons.

> *"Our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."*

The Directive aligns data protection standards of US persons and foreign citizens and residents in terms of proportionality elements, security safeguards, and includes internal executive branch oversight. However, several safeguards that the Presidential Policy Directive makes available for non-US persons are of a minimal standard and it is questionable whether the Directive actually increased data protection safeguards for EU citizens (Bignami, 2015).

In contrast to Presidential Policy Directive-28 and the Judicial Redress Act, the FREEDOM Act (2015) primarily strives to improve data protection safeguards of US persons in the contexts of law enforcement and foreign intelligence activities and thereby amplifies the distinction of data protection standards which is also included in the FISA Act, Executive Order 12,333 and within application of NSLs.

Summarized, the US data protection framework does not constitute a comprehensive framework. Data protection safeguards are included in various legal Acts which leads to a fragmented and inextricable amount of rights on data collection and data protection. The only two legal measures that could grant a comprehensive protection of personal data are subject to various limitations, particularly regarding law enforcement and surveillance within the realm of national security. Additionally, the rights within the Privacy Act and the Fourth Amendment almost always exclude non-US persons from their scope. However, the Judicial Redress Act and the Umbrella Agreement do present some improvements for the data protection rights of EU citizens in the US.

3.3 Conclusion

Within this chapter the different feature of the EU and the US data protection frameworks have been identified and analysed. The analysis yields that the European Union and the United States differ in the nature, scope and extent to which they protect personal data.

On the one hand, the EU data protection framework constitutes a comprehensive framework in which the right to the protection of personal data displays a fundamental right that is protected within EU primary law and; therefore, a right at the top of the norm hierarchy within the EU. The US data protection framework, on the other hand, neither displays a comprehensive framework nor does it include constitutional protection of the right to data protection that is comparable with the status of the right as a fundamental right within the EU. Even though the Fourth Amendment does imply the protection of personal data, the right to data protection is not specifically protected as is the case in Article 16 TFEU and Article 8 CFREU which have been discussed in chapter 2.1. In terms of comprehensiveness, the Privacy Act's provisions are most comparable to the EU data protection framework. However, neither the Privacy Act not the Fourth Amendment apply to non-US person, thus excluding EU citizens from their scope. Also, in the case of the SWIFT Agreement, neither the Fourth Amendment nor the Privacy Act set any regulations on data collection because the former permits data sharing for law enforcement purposes, and provisions of the latter do not apply because of the 'third party doctrine' as discussed in chapter 3.2.

The exclusively of the US data protection rights and safeguards for US persons stands in contrast to the EU data protection framework which is not excluding any individual from its protective measures and remedies. This is in line with the European perception of privacy as an aspect of dignity that is to be granted every human being and is not to be limited to citizenship. The fact that the right to data protection constitutes a fundamental right in the EU also fits into this picture. The US data protection framework displays the American perception of privacy as an aspect of liberty from the state. Rights to the liberty from the state are inter alia limited by the duty of the state to ensure the security of its citizens which represents one of the state's most important justifications for its existence. Therefore, it is hardly surprising that the protection of personal data in the US is exposed to extensive restrictions and the extensive possibilities for law enforcement and national security agencies to collect personal data via several Acts, such as the USA PATRIOT Act and the FISA Act.

Two terminologies within the data protection frameworks are exemplary for the different data protection standards across the Atlantic. In the EU, the concept of proportionality and necessity takes the most important position in the context of data protection and security. Based on this concept, European Courts have been analysing in a strict way whether or not any action that limits the right to data protection is proportionate and necessary. In contrast, the US makes use of another term in its legislation, namely the term reasonableness. While the terms proportionality and reasonableness both include normative aspects, the term proportionality presupposes that a balance needs to be created between surveillance for security purposes and data protection. In the past, the European Courts have often decided in favour of the right to data protection. The term reasonableness in the US, however, justifies limitations to the protection of personal data when it is appropriate for a purpose of the agency that aims to collect that data. This does not necessarily include an assessment of whether or not the limiting action also stands in proportion to its aim. Reasonableness in the EU is a mere part of the test of necessity and proportionality and only comes before the actual proportionality is being tested.

Especially since 9/11 due to the extensions of surveillance possibilities for law enforcement agencies in course of the PATRIOT Act, it becomes apparent that the US's focus in the relationship of security and privacy lies on security aspects, and that the US legal framework provides for lower data protection standards than the data protection framework in the EU. This creates a problem for the protection of personal data under the SWIFT Agreement if the Agreement does not provide sufficient rights and safeguards regarding the transfer of data that are consistent with the EU data protection standards.

4. Data Protection within the EU-US SWIFT Agreement

The differences in the data protection frameworks make it feasable that EU citizens' personal data which are transferred from EU to US territory in the context of the SWIFT Agreement might not be protected in a way that is consistent with EU data protection standards. The aim of this chapter is to analyse whether the SWIFT Agreement provides for a level of data protection that is consistent with the data protection provisions within EU treaties. Therefore, this chapter will first provide a historical background of the formation of the SWIFT Agreement (SWIFT-II Agreement), including the role of relevant actors. Since this analysis will include two smilar agreements which have been concluded on the TFTP, the SWIFT Agreement will be referred to as SWIFT-II Agreement. The interim agreement that preceded the SWIFT Agreement will be referred to as SWIFT-I Agreement.

The historical review is followed by an analysis of the SWIFT-II Agreement regarding its structure and its data protection provisions. A summary of existing critique on the permanent SWIFT agreement will give further insight in order to answer whether or not the SWIFT-II Agreement provides for a protection of personal data that is in accordance with the EU data protection standards.

4.1 Historical Background: TFTP and SWIFT I

In the aftermath of the 9/11 terrorist attacks, the US Department of the Treasury (UST) initiated the so-called Terrorist Finance Tracking Program (TFTP) with the aim to "identify, track, and pursue terrorists (…) and their networks" (U.S. Department of the Treasury, n.d.). The strategy of the TFTP is to access data of the Belgian based Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a cooperative institution established by financial institutes and handles the vast amount of the worlds trans-border financial payment messages transfers. On the current "peak day" of 2018, SWIFT counted a total of 35,223,536 messages (SWIFT FIN Traffic & Figures, n.d.).

These messages can include personal data such as the name of payer and payee (Servent & MacKenzie, 2012). This does not only make these data valuable for governmental law enforcement agencies in the fight against terrorism but also makes any transfer of that data an issue of data protection. SWIFT stored financial messaging data of EU citizens not only in the territory of the EU but also saved a copy of that data on a second server on US territory (Virginia), in a so called 'mirroring system'. Therefore, SWIFT had to comply both with EU data protection legislation and US law which allowed the UST to request and receive SWIFT's

financial messaging data via administrative subpoenas in a way that was compatible with U.S. law. This practice, however, makes the TFTP a crucial program in the transatlantic relationship and for EU data protection because, as has been observed in chapter 2 of this analysis, EU and US have different data protection frameworks and the EU possesses higher data protection standards. Therefore, action that is compatible with US law on data protection is not automatically compatible with EU data protection law and EU data protection standards, too.

In addition, the TFTP was kept secret until the New York Times revealed its existence on 23 June 2006 (Exten, 2006). While the UST assured that the TFTP was in accordance with the law, the European Union saw the possibility that the program might violate and undermine EU citizens' data protection rights (Exten, 2006). In its February 2007 resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (February 2007 Resolution), the EP voiced its concern:

> *"over the fact that for four years SWIFT, upon receipt of subpoenas, has been transferring to the US administration a subset of data treated in its US systems, including data that did not concern US citizens and data not generated on US"*
> (European Parliament, 2007)

The EP found that the TFTP was in violation with the fundamental rights to data protection assured for in the ECHR, the CFREU, EU primary law treaties as well as the then valid secondary law. Consequently, the EP proposed in its February 2007 Resolution that SWIFT should change its current practices, especially in terms of its mirror server in Virginia (European Parliament, 2007, paragraph 21). This led SWIFT to move all data concerning EU citizens to a new server in Switzerland, thereupon making it illegal for the UST to request EU citizen's financial messaging data via administrative subpoenas (Servent & MacKenzie, 2012).

However, both EU member states and the EP recognized the benefits of a TFTP to counter terrorism. Especially the EU member states feared disadvantages due to their exclusion of the US TFTP (Servent & MacKenzie, 2012), and the EP pronounced in its February 2007 Resolution that it "believes that the EU and the US are fundamental and loyal allies in the fight against terrorism and that this legislative framework should therefore be the basis for the negotiations of a possible international agreement" (European Parliament, 2007). However, while the EU member states' focus in terms of this possible transatlantic TFTP agreement was focused on the security aspect, the EP has probably also seen a great opportunity in this agreement for the promotion of data protection standards.

After the Council gave a negotiation mandate to the Presidency and the Commission on 27 July 2009 it took merely four months for the negotiations to produce a result. On 30 November 2009 an interim agreement (SWIFT-I) was concluded (European Parliament, 2010). The timing of SWIFT-I, however, gave ground to a lot of criticism by the EP: On 1 December 2009, the following day, the Lisbon treaty entered into force, granting the European Parliament the right to co-decide on the adoption of international agreements. Regarding the adoption of SWIFT-I, the EP not only felt side-lined but was furthermore concerned about the level of data protection within the agreement (Servent & Mackenzie, 2012). When the EP was given the opportunity to vote on the agreement on 11 February 2010 it rejected the SWIFT-I Agreement which was subsequently annulled (European Parliament, 2010).

Nevertheless, negotiations on a new permanent SWIFT agreement (SWIFT-II) were initiated shortly afterwards by the Commission and approved by the Council on 10 May 2010 (European Parliament, 2010). However, according to Servent and MacKenzie (2012), negotiations on the permanent SWIFT-II agreement succeeded due to a change in US strategy and not due to a fundamental change of the content of the agreement. The most important change in this sense was to give EU actors a more important role during the negotiation process and to follow a strategy of dialogue rather than lobbying. Accordingly, the EP had the chance to introduce changes and thereby to increase the "fit" of the agreement. Even though SWIFT-II did not fundamentally differ from SWIFT-I, the better inclusion of the EP and the acceptance of some changes regarding the protection of personal data made it possible for the EP to justify an approval to the agreement. As a result, the EP passed the agreement in its vote of 8 July 2010.

Servent and MacKenzie (2012) furthermore claim that the EP and the EU acted as norm takers within the SWIFT-II negotiations, therefore, taking the same roles as they did in previous negotiations on transatlantic data sharing agreements prior to the Lisbon treaty. This makes the SWIFT-II negotiations even more chastening because during these negotiations the 'data protection promoting EP' had, for the first time, been able co-decide on an international data sharing agreement, and the EU had a greater leverage when compared to negotiations on the PNR agreement because SWIFT-data were located on the territory of the EU. These two characteristics of the SWIFT-II negotiations could have given the EU, the EP in particular, the opportunity to include high data protection standards in the agreement and to act as norm makers rather than norm takers within the negotiations with the United States. The fact that neither the EU nor the EP did act as norm makers even more highlights the continuing norm

taking role of the EU in negotiations on transatlantic data sharing agreements within the realm of security and counter-terrorism approaches (Servent & MacKenzie, 2012).

4.2 SWIFT II

The SWIFT-II Agreement consists of a Preamble which is followed by 23 Articles (European Union & United States of America, 2010). The Preamble is emphasising both the fundamental right to data protection as entailed in EU primary law as well as the importance and success of the TFTP to combat terrorism and its financing in the world and, in particular, in the EU. It is inter alia specifically referred to the Council of Europe Convention No. 108 and Articles 6(2) TEU, 16 TFEU, 8 ECHR, and 7 and 8 CFREU. Overall, a focus on cooperation can be observed throughout the Preamble and the Articles of the Agreement, for example, by reference to a "transatlantic partnership", to "jointly" coordination, to "common values and principles" and to the "mutual sharing of information" (Preamble). Within the Preamble of the SWIFT-II Agreement, the important role of the EU for the maintenance of the TFTP in terms of data transfers from EU to the UST is specifically highlighted.

The objective of the SWIFT-II Agreement, as laid down in Article 1, is to ensure both the transfer of financial messaging data from EU territory to the UST as well as to provide "relevant information obtained through the TFTP" to government authorities of Member States, Europol, or Eurojust, in order to combat terrorism and its financing (Article 1(1)). In the following, the SWIFT-II Agreement will be systematically analysed in terms of the consistency of its data protection rights and principles with the EU data protection framework as analysed within chapter 2.1 of this study.

4.2.1 Data Transfer Procedure

The procedure for the data transfer which is the purpose of the Agreement is outlined in Article 4, as well as in Articles 9 and 10 of the SWIFT-II Agreement. Accordingly, to receive financial messaging data, the UST is required to send a request that contains a purpose limitation to the Designated Provider[7] and "simultaneously (to) provide a copy of the Request (…) to Europol" (Article 4(2), (3)). Europol is then asked to verify that the request includes clear definitions of both the requested data and the necessity of that data for the purpose of

[7] A Designated Providers are "providers of international financial payment messaging services" (Article 3 SWIFT-II Agreement)

processing, that it does not seek to process data relating to the Single Euro Payments Area and that the request is as narrowly tailored as possible (Article 4(2)). If this is the case, Europol notifies the Designated Provider of the verification (Article 4(4)) and thereby, the request has "*binding legal effect as provided under US law, within the European Union as well as the United States*" (Article 4(5)).

The means that US law is given full applicability within EU territory, and furthermore that the Designated Provider is then "authorised and required to provide the data (directly) to the U.S. Treasury Department" (Article 4 (5), (6)). Not only is US law granted full applicability in EU territory but "Designated Providers shall have all administrative and judicial redress available under U.S. law to recipient of U.S. Treasury Requests" (Article 4(8)). Therefore, it clearly becomes obvious that US law is given a predominant stand in the data transfer procedure as outlined in Article 4 of the Agreement. Despite one European control authority – Europol – the EU is completely subordinating itself to the US and the US legal system, therefore clearly acting as a norm taker in this aspect of the SWIFT-II Agreement.

4.2.2 Data Protection Rights and Principles

Nearly half of the Articles within the SWIFT-II Agreement contain provisions aiming to protect the data that is being transferred from the territory of the EU to the UST for the purpose to counter terrorism and its financing (Articles 5-8 and 14-17). In the following, these provisions are analysed within the categories that have been identified in chapter 2.2.3: Lawful processing, transparency, control and review mechanisms and effective remedies.

The SWIFT-II Agreement provides for the prerequisite that the application of all the provisions takes place without any form of discrimination, especially by virtue of nationality or country of residence (Article 5).

4.2.2.1 Lawful Processing

The data protection principles for lawful processing as well as the purpose limitation principle are codified in Article 5 of the SWIFT-II Agreement. According to Article 5(1) lawful data processing requires that it takes place in accordance with the provisions of the agreement and is furthermore necessary to achieve its legitimate purpose of "the prevention, investigation, detection, or prosecution of terrorism or its financing" (Article 5(1)).

The SWIFT-II Agreement furthermore provides for data quality principles. Searches of the Provided Data[8] and retention of that data must meet the requirements of necessity and proportionality. The searches must demonstrate that they are based on existing information or evidence that adequately link the data subject with a terrorist act and be "narrowly tailored" and logged (Article 5(3)). The Agreement furthermore provides for regular evaluations by the UST at intervals of no more than one year to ensure the relevance of the data, namely to detect "non-extracted data that are no longer necessary to combat terrorism or its financing" and to "asses the data retention period" based on necessity (Article 6(1), (5)). Provided Data or retention periods that no longer meet the requirement of necessity have to be "permanently delete(d) as soon as technologically feasible" or decreased respectively. The Parties to the Agreement also have to make sure that the data that is being stored contains accurate information and prevent any reliance on inaccurate or otherwise erroneous data (Article 17(1)).

Provided Data is furthermore subject to several requirements how it has to be stored and to limitations on who gets authorised access to the data in order to ensure its security and to assure accountability (Article 5(4)a)-e)). Onward transfers are regulated within Article 7 of the SWIFT-II Agreement. Accordingly, Provided Data can be shared "with law enforcement, public security, or counter terrorism authorities in the United States, Member States, or third countries, or with Europol or Eurojust, or other appropriate international bodies, with the remit of their respective mandates" (Article 7(b)). The onward transfer is furthermore coupled to the purpose limitation as outlined in Article 5(1) and must be aimed at leads, be in consent of the competent authorities of the Member State concerned, be stored no longer than necessary by the recipient authority and be duly logged (Article 7 (c)-(f)).

In sum, the Agreement couples the processing and onward transfer of personal data to data quality principles and to the principle of necessity and proportionality. The provisions of the SWIFT-II Agreement take account of the importance of the principle of proportionality and necessity for data retention periods in the EU in that the retention period has to be assessed annually in terms of its necessity. The importance of a proportionate retention period has been highlighted in the ECJ judgment on the Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (Digital Rights Ireland case), in which the ECJ

[8] Provided Data in the SWIFT-II Agreement are defined as "requested financial payment messaging and related data which are necessary" to combat terrorism and its financing and which are provided by Designated Providers to the UST for this purpose (Article 3 SWIFT-II Agreement)

invalidated Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks" (Data Retention Directive) (European Parliament and Council of the EU, 2006). The ECJ justified its decision with the explanation that the provisions on retention within the Data Retention Directive did not comply with the principle of proportionality in that it did not "sufficiently circumscribe (…) interference to ensure that it is limited to what is strictly necessary for the purpose of fighting 'serious crime', thereby leaving it too open for Member States to decide on the scope of data retention" (Article 29 Data Protection Working Party, 2014b).

However, the assessment of the data quality (relevance, necessity) and of the data retention period's necessity fall within the remit of the UST. Again, data protection has been outsourced to the United States who possess lower data protection standards than the EU. Therefore, it cannot be assured by the provisions of the SWIFT-II agreement that the relevance and necessity of the data and the retention period are provided in alignment with EU standards and according to the strict proportionality and necessity tests of the ECJ. The provisions of the SWIFT-II Agreement on fair processing for a specific purpose seem to comply with the principles of Article 8(2) CFREU and Article 8 ECHR at first glance. Nevertheless, the lower data protection standards of the US and the norm taking role of the EU who lets the UST the power to review and to assess the necessity to keep on storing personal data of EU citizens leaves questions regarding the consistency of SWIFT-II data protection provisions with EU data protection standards. Also, the authorities with whom the personal data can be shared covers a very broad range, including Europol. Therefore, Europol, the only pre-transfer controlling authority, also benefits from the transfer of data in the context of the SWIFT-II Agreement.

4.2.2.2 Transparency

The principle of transparency encompasses the right to know about the processing of one's personal data (Article 14), the right of access (Article 15) and the right to rectification, erasure or blocking (Article 16). Upon request, the SWIFT-II Agreement grants "any person" the right to obtain "confirmation (…) as to whether that person's data protection rights have been respected" regarding the data protection provisions of the Agreement (Article 15(1)). The right to access the information, however, can be reasonably limited by national law for public or national security purposes (Article 15(2)). It must be emphasised at this point that both EU member states and especially the US expanded their anti-terror legislation in the aftermath of

the 9/11 attacks. Despite the fact that a limitation requires a written explanation and "information on the means available for seeking administrative and judicial redress in the United States" (Article 15(3)), the possibility to limit the right to access for national security reasons could proof to restrain the right to access for EU citizens, especially in the territory of the United States, extensively. The limitation becomes even more striking when viewed in combination with the fact that administrative and judicial redress are only available under US law. Article 16 of the SWIFT-II Agreement provides a person with the right seek rectification or erasure of processed personal data as well as to block data processing in case he or she believes the processed data is inaccurate or the processing undermines the provisions of this Agreement (Article 16).

The right to access implies that the person whose data is being processed knows about the processing and the right to rectification, erasure or blocking of processing requires that the data subject possesses further information, for example on the purpose of processing and the fact that he has those rights. Therefore, how to exercise the rights of access, rectification, deletion and blocking of Articles 15 and 16 by means of "administrative and judicial redress as appropriate in the United States regarding the processing of personal data received pursuant to this agreement" as well as detailed information on the TFTP and its purposes must be published by the UST on its public website to ensure transparency (Article 14(1)).

In sum, Articles 14 to 16 of the SWIFT-II Agreement include several provisions to grant "any person", thus irrespective of nationality or country of residence, the right to access and to request rectification of processed data concerning him or her and require the UST to ensure for the knowledge of the data subject on the purposes of their data processing within TFTP and further information on that processing. However, the right to access is subject to a drastic limitation for national security reasons when considering the wide applicability of exceptions in the context of national security in the USA since 9/11. Again, there is a clear dominance of US law as the possibilities for redress are only available under US law and it is in the hands of the UST to rectify, erase or block inaccurate data or data that has been processed in contradiction to the SWIFT-II Agreement. Finally, it is not sure whether the right to access will be made available and can be effectively enacted by EU citizens in the United States. Therefore, the rights of EU citizens who seek access and rectification of their data as required by Article 8(2) of the CFREU could be limited by the national security exception and especially by the missing redress possibilities under EU law.

4.2.2.3 Control and Review Mechanisms

Articles 12 and 13 of the SWIFT-II Agreement provide for control and review mechanisms. It is required for "independent overseers", authorized to monitor both in real time and retrospectively the compliance with the data protection safeguards of Articles 5 and 6 of the Agreement (Article 12(1)). These overseers include a person that is appointed by the European Commission and are, according to Article 13 of the Agreement, themselves subject to a Joint Review by the European Commission and the UST. In addition, the Joint Review is intended to examine the "implementation and effectiveness of this agreement" and the "compliance with data protection obligations specified in this agreement". The SWIFT-II Agreement furthermore provides for a proportionality assessment of Provided Data, "based on the value of such data for the investigation, detection, or prosecution of terrorism or its financing" (Article 13(2)).

But even though the SWIFT-II Agreement does include "independent" oversight, it can be criticised that it is not provided for any form of judicial oversight by the European courts. Due to the fact that the SWIFT-II Agreement is an executive Agreement, it is not provided for any sort of judicial review in the United States (Servent & Mac Kenzie, 2012). Europol displays the only pre-control within the data transfer to control UST-requests to prevent bulk data transfer or any transfer which is not necessary and proportionate to achieve the purpose of countering terrorism and its financing. However, the inclusion of Europol was nevertheless a concession of the EP "who called for a public judicial body to review US requests and not for a public law-enforcement body such as Europol (…) (whose) analysists assess US requests 'in the light of operational considerations and security needs'" (Amicelle, 2013, p.11). Furthermore, as a police cooperation agency, it is itself profiting from the data exchange in the context of the SWIFT-II agreement and could therefore be biased. The retrospective control mechanism in form of the joint review by the Commission and the UST give ground to similar criticism. Both the Commission and the UST might be biased in conducting the Joint Review because they are in favour of the cooperation in TFTP data sharing in order to combat terrorism.

4.2.2.4 Available Remedies

The right to be informed of the possibility to seek administrative or judicial redress is ensured for within Articles 14, 16. The right to redress, however, is specifically addressed in Article 18 of the SWIFT-II Agreement which reads as follows:

> "*Any person who considers his or her data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively. For this purpose (…) the U.S. Treasury Department shall treat all persons equally in the application of its administrative process, regardless of nationality or country of residence. All persons, regardless of nationality or country of residence, shall have available under U.S. law a process for seeking judicial redress from an adverse administrative action*."

Article 18 therefore grants both EU and US citizens the right to seek administrative and judicial redress. This can be considered a progress to US law which excludes non-US persons from such a possibility. Nevertheless, the administrative and judicial redress are only available under US law and is therefore bound to US data protection standards which are less extensive than EU data protection standards. This displays a clear dominance of the US. It is questionable whether the right to access, rectification, erasure and blocking will be made available for EU citizens under the law of the United States which excludes EU citizens from most data protection provisions.

4.3 Conclusion

While the joint reviews by UST and Commission draw positive conclusions on the TFTP and the SWIFT-II Agreement, the EP continues to be critical. Its concerns over the SWIFT-II Agreement were compounded by the revelations by Edward Sowden in 2013[9]. This led the European Parliament to its *resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency* surveillance in which it states that the press reports indicate that the NSA surveillance included direct access to financial payment messages of SWIFT (European Parliament, 2013). Furthermore, the EP states in this resolution that "the Agreement has not been implemented in accordance with its provisions, in particular those laid down in Articles 1, 4, 12, 13, 15 and 16" (European Parliament, 2013, Article 6).

[9] The former CIA employee and contractor for the U.S. government leaked classified information from the NSA on the mass surveillance of internet and telecommunication companies which involved the personal data of millions of customers and inter alia of EU citizens. The surveillance took place based on an order under the FISA Act which had been established in the aftermath of the attacks on 9/11 (Beuth 2016; Greenwald, 2013)

Accordingly, in the opinion of the EP it is neither provided for the transparency provisions nor for the control and review mechanisms of the SWIFT-II Agreement. Since the SWIFT-II Agreement has not been amended or suspended, the EP's criticism continues within its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, and its resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (European Parliament, 2014; European Parliament, 2015.

Contrary to the conclusions of Servent and MacKenzie (2012), the SWIFT-II Agreement emphasises the cooperation of equal partners in its Preamble. This would suggest that EU data protection standards form an important part of the agreement. The SWIFT-II Agreement displays an improvement to the SWIFT-I agreement in terms of the inclusion of formal data protection safeguards (Pfisterer, 2010; Servent & MacKenzie, 2012). The previous analysis within chapter 4.2.2 showed that the SWIFT-II Agreement formally includes the rights and principles of the categories 'lawful processing' and 'transparency.' The rights and safeguards within these categories are consistent with EU data protection standards since it is assured for purpose limitation, data quality standards, a secure storage of the data and the rights to access, rectification, erasure and blocking of data processing. The analysis has shown that the SWIFT-II Agreement also takes account of the concept of necessity and proportionality, especially regarding a limitation of the data retention period (4.2.2.1).

Nevertheless, it is not clear whether these rights are really made available to EU citizens. As has been analysed within chapter 4.2.4, any administrative or judicial remedy for a person who considers his or her data protection rights to be violated is located within and is therefore bound to US law. It is questionable whether the SWIFT-II Agreement's rights would actually trump the Fourth Amendment and the Privacy Act from 1974 which exclude non-US persons from most data protection provisions. Even if the rights are made available to EU citizens, they will have to be enacted under the US data protection framework which has been found throughout this study to have significantly lower data protection standards than the EU (Chapter 2.3). The fact that the US data protection framework is marked by exceptions in favour of national security that are justified via the concept of reasonableness is particularly illustrated by the NSA affair. Also, within the SWIFT-II Agreement, the right to access is subject to a drastic limitation for national security reasons, especially when considering the far-reaching expansion of exceptions by the USA PATRIOT Act in the US since 9/11.

Furthermore, the transfer of bulk data from the EU to the UST remains a sticking point despite the purpose limitation principle and the requirement of narrowly tailored requests by the UST (see Chapter 3.2.2). Nonetheless, "each request covered several weeks and several geographic areas" and due to the high amount of data traffic that is handled by SWIFT it can be estimated that the UST "collected several hundred million messages during five years (Amicelle, 2013, p.14). Therefore, the SWIFT-II Agreement cannot be said to preclude bulk data transfers from the EU to the US.

Last but not least, also the design of the control and review mechanisms is not consistent with EU data protection standards. Europol displays the only pre-transfer control. Europol, however, might be subject to bias since it is itself an agency that benefits from the data transfer within the SWIFT-II Agreement. The same holds true for the joint review by the Commission and the UST which have both been in favour of the SWIFT Agreement in the past.

Therefore, while the SWIFT-II Agreement includes formal data protection rights and safeguards which display an improvement to the SWIFT-I Agreement, the SWIFT-II Agreement does not provide for substantial rights and safeguards in consistency with EU data protection standards. All of the formal rights are limited by the fact that EU citizens are only granted judicial and administrative redress possibilities under US law and therefore within the US data protection framework which does not provide for the same standard if data protection as the EU. Now it remains to be seen whether the newly introduced LE Directive impacts the protection of personal data of EU citizens within transatlantic data sharing agreements and data transfers to third states.

5. The Law Enforcement Directive

The following chapter will take account of the recent developments within EU secondary law on data protection - the "body of law that comes from the principles and objectives of the treaties" and therefore from data protection principles of the ECHR, the CFREU and the EU Treaties as outlined in chapter 2.1 of this research (European Commission, 2018a). In 2016, the European Union adopted a new data protection reform package in order to meet the new needs that are triggered by technological developments of the digital age. The reform package includes a regulation (Regulation (EU) 2016/679, subsequently the "GDPR") which repeals Directive (EU) 95/46/EC (the Data Protection Directive) and sets general data protection rules, and a Directive (Directive (EU) 2016/680, subsequently the "Law Enforcement Directive" or "LE Directive") which repeals Council Framework Decision

2008/977/JHA (Council Framework Decision) and addresses the JHA and law enforcement sector. Since this research focuses on data protection within the realm of counter-terrorism, the LE Directive represents the core of this chapters' analysis.

GDPR and LE Directive not only differ in their scope but also in the very nature of their instrument. While the GDPR is a binding legal act which is applying "automatically and uniformly to all EU countries" from the moment it enters into force, the LE Directive only sets minimum requirements for the EU Member States, leaving it to them to choose how to transpose the Directive into national law (European Commission, 2018a). The difference originates from the special nature that the EU assigns to the JHA which is also highlighted by declaration 21 to the TFEU on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation where it is stated that "*specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 B of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields*" (European Union, 2012d, p. 326). By 6 May 2018 the EU member states had to have transposed the LE Directive into national law and 19 days later, on 25 May 2018, also the GDPR entered into force (General Secretariat of the Council, 2017).

Within the chapter 4 it has been concluded that the SWIFT Agreement, while formally providing for EU data protection principles and safeguards, is not consistent with EU data protection standards in case of its substantial protection of personal data. The aim of this chapter is to analyse the extent to which the SWIFT Agreement and the LE Directive build a consistent legal framework for the protection of personal data of EU citizens.

5.1 Scope and Objective of the Law Enforcement Directive

In Articles 1 and 2, the LE Directive lays down its scope and the objective which are furthermore accomplished by several paragraphs referred to prior to the Articles of the LE Directive. The scope of the LE Directive is an improvement compared to the preceding data protection legislation in the context of transatlantic data sharing for counter-terrorism purposes. While the Data Protection Directive did not apply to the JHA sector of the pre-Lisbon pillar structure at all, the Council Framework Decision applied to this sector but only regulated data transfers within the EU (Paragraphs (5) and (6)). Article 1 and 2 hold that the LE Directive

addresses processing of personal data by competent authorities[10] within the realms of law enforcement and public security and Chapter V of the LE Directive encompasses rules on the data transfers to third countries and international organisations. Nevertheless, the applicability of the LE Directive is limited to actions that fall within the scope of Union law and to data processing by competent authorities of EU member states, excluding data processing by "Union institutions, bodies, offices and agencies" (Article 2). The LE Directive also does not apply to the whole territory of the EU since the United Kingdom, Denmark and Ireland are excluded from its scope (Paragraph 99 and 100). The scope does, however, extend beyond EU territory to competent authorities of Liechtenstein, Norway and Switzerland because the LE Directive develops the provisions of the Schengen acquis[11] (Paragraphs 102 and 103).

The objective of the LE Directive is to contribute to the AFSJ and to "protect the fundamental rights and freedoms of natural persons and in particular the right to the protection of personal data" while ensuring the transfer of personal data between EU member states but also between the EU or EU member states with third countries (Article 2 (a) and (b); also see Paragraphs (2), (4), (7) and (93)). Furthermore, the LE Directive aims to strengthen and to improve the coherence of the EU data protection framework by providing harmonised rules with a high level of protection of personal data for EU member states in the sector of law enforcement and public security (Paragraphs (4), (7) and (15)).

5.2 Data Protection Rights and Principles

The data protection provisions of the LE Directive align to the principles as set out in the ECHR and in EU primary law and case law of the ECtHR and the ECJ (Paragraphs (46), (104)). This is specifically emphasized within paragraph (104) which reads as follows:

> *"This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private*

[10] Competent authorities are defined in Article 3 of the LE Directive as "any public authority competent for, (…) or any other body or entity entrusted by Member States law to exercise public authority and public powers, for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security"

[11] Schengen Agreement of 1985, Schengen Convention and related agreements and rules that have been integrated into the framework of EU legislation in 1999. The Schengen acquies lays down the rules on the Schengen area. The Schengen area guarantees the free movement of persons without internal border controls ("Glossary of Summaries. Schengen (Agreement and Convention)")

and family life, the right to the protection of personal data, the right to an effective remedy and to fair trial."
(European Union & Council of the EU, 2016a, p.105)

Data protection principles and the rights of the data subject are codified in Chapters II and III of the LE Directive respectively. In order to be able to compare the data protection principles and rights provided for within the LE Directive with the SWIFT-II Agreement, the principles and rights will, again, be classified according to the categories that have been identified in chapter 2.2.3: Lawful processing, transparency, control and review mechanisms and effective remedies.

5.2.1. Lawful Processing

Article 4 lays down principles for the processing of personal data and data quality standards which are both further specified within Chapter II and III of the LE Directive. Processing of personal data is required to occur only "for specified, explicit and legitimate purposes and not (…) in a manner that is incompatible with those purposes" (Article 4). The purpose for data processing within the scope of the LE directive is further limited to "*purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*" (Article 1 (1)). Article 4 of the LE Directive furthermore requires that processing of personal data is fair and in accordance with the law (Article 4 (1) (a)). The principle of fair processing is specified in paragraph (26) and includes to inform natural persons "of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing". A whole other article in the LE Directive is dedicated to the lawfulness of processing (Article 8). Article 8 links the lawfulness to the principle of proportionality and the purpose limitation principle in that any processing must be necessary for the duty of a competent authority regarding its purpose as defined in Article 1 (1).

The personal data which is being processed should be "adequate, relevant and not excessive in relation to (and not longer than necessary for) the purposes for which they are processed" (Articles 4 (1) (c) and 5). Article 7 adds that it must be ensured by the competent authorities that "personal data which are inaccurate, incomplete or no longer up to data are not transmitted or made available". In case that the processed data is incomplete, incorrect or incompatible with the provisions of Articles 4, 8 or 10 of the LE Directive, the data subject can request completion, correction and erasure of that personal data (Article 16 (1), (2)). In case

that neither the accuracy nor inaccuracy of the personal data can be determined, the controller is required to restrict the processing (Article 16 (3) (a)).

Additionally, the LE Directive requires that it is assured for the data's accuracy and security (Article 4 (1) (d), (f); also see paragraph (28), (30), (32)).

The provisions of the LE Directive regarding a lawful processing, including purpose limitation, provisions on data quality and the right to accurate data, are consistent with the data protection rights provided for in the SWIFT Agreement as outlined in chapter 4.2.2.1 of this study.

5.2.2 Transparency

The data subject has the right to obtain information on and access to his or her personal data that is being processed from the controller (Article 14). The right to access requires that the data subject knows of the processing of his or her personal data in the first place. Therefore, according to Article 12 and 13, the minimum of information that the controller must provide the data subject with are the controller's identity, the purposes for which he or she intends to process the personal data, contact details of controller, data protection officer and supervisory authority, as well as the rights of the data subject to request access, rectification, erasure or restriction of processed personal data (Article 12 (1), 13 (1)). This information should be given in a clear and easily understandable language and be easily accessible, for example on the website of the controller (Article 12 (1), paragraph (42)).

The SWIFT Agreement is compatible with the LE Directive also in terms of the transparency provisions it provides, and which have been outlined in detail in chapter 4.2.2.2.

5.2.3 Control and Review Mechanisms

Article 4 (5) – review of lime limits for storage

Within the LE Directive, independent supervisory authorities occupy an important position, to which the entire 6th chapter of the Directive is dedicated. "*Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union*" (Article 41 (1)). In particular, the importance of independence is emphasized. Any possible external influence on the members of the supervisory authorities has to be foreclosed and they must be appointed in a transparent procedure (Articles 42, 43). The supervisory authorities are requested to inter alia "check the lawfulness of processing", "conduct

investigations on the application" of the LE Directive and to "monitor relevant developments insofar they have an impact on the protection of personal data, in particular the development of information and communication technologies (Article 46 (g), (i), (j)). Additionally, they have the power to investigate controller and processor regarding their access to personal data that they process (Article 47 (1)).

The Board which has been established by the GDPR is also required to examine questions relating to the application of the LE Directive and "issue guidelines, recommendations and best practices in order to encourage consistent application" (Article 51 (b)). It is also involved in the transfer of personal data to third countries in that it provides the Commission with its opinion on whether or not the country in question possesses an adequate protection of personal data (Article 51 (g)).

In the context of the LE Directive, the Commission has to lodge a review and transfer it to EP, the Council of the EU and publish it (Article 62). According to paragraph 2 of this Article, the review has to pay special attention to personal data transfers to third countries.

5.2.4 Effective Remedies

Remedies available under the LE Directive are codified in Chapter VIII. Therein it is provided for the "right to lodge a complaint with a supervisory authority" and the" right to effective judicial remedy against a supervisory authority" (Article 52, 53). Such a complaint can be lodged by any data subject who is of the opinion that the processing of his or her personal data is in violation to data protection provisions outlined in the LE Directive (Article 52 (1)). The data subject then has also the right to an effective judicial remedy both against a legally binging decision of a supervisory authority as well as in case that the data subject is not informed of the progress and outcome of the complaint within three months or the complaint has not been handled by the competent supervisory authority at all (Article 53(2)). Furthermore, any natural or legal person has the right to effective judicial remedy in the case they consider the data processing to be infringing their rights under the LE Directive (Article 54). What is outstanding is the fact that the LE Directive provides for the right to compensation in Article 56 for any person, thereby not excluding any non-EU national and setting forth the far-reaching applicability of the data protection safeguards within the European Union. Accordingly, anyone who has been damaged due to any unlawful processing pursuant to the LE Directive's data protection provisions, is obliged to receive compensation for that damage from either the controller or another competent authority under member state law.

5.3 Data Transfers to Third Countries

Article 35 of the LE Directive holds that personal data can only be transferred to a competent authority of a third country if necessary for the purpose as outlined in Article 1(1). Furthermore, the country in which the competent authority is located must either possess an adequate protection of personal data that is certified by an adequacy decision of the Commission - inter alia taking into account the respect for human rights and fundamental freedoms, relevant legislation and its implementation, data protection rules, the existence of independent supervisory authorities and of effective and enforceable data subject rights and remedies in the third country - or be subject to appropriate safeguards "provided for in a legally binding instrument" or ascertained by the controller after assessment of the circumstances concerning the transfer (Article 35 (1) (d); Article 36 (1), (2) (a), (b); Article 37 (1) (a), (b)); or summarized in paragraphs (64), (67), (71)). In paragraph 74, the LE Directive acknowledges that data transfers to third countries "may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data" and may pose problems due to "insufficient preventative or remedial powers of inconsistent legal regimes.

5.4 Conclusion

The LE Directive and the SWIFT Agreement are consistent in their formal data protection principles and rights regarding the processing of personal data. The "specified, explicit and legitimate purpose" of the SWIFT Agreement which the LE Directive requires in Article 4 is "the prevention, investigation, detection, or prosecution of terrorism or its financing" (Article 5(1) SWIFT Agreement). The SWIFT Agreement furthermore provides for the data quality standards that are required by the LE Directive in Article 4. Also, the transparency requirements which are included in the LE Directive in line with EU primary law are met by the SWIFT Agreement as the UST publishes information on the TFTP program and on the administrative and judicial redress possibilities on its website and the SWIFT Agreement provides for the rights to access, rectify, and erase inadequate, incomplete or unlawfully processed data.

Nevertheless, the nature of the redress possibilities to enact all these rights constitutes an inconsistency between the LE Directive and the SWIFT Agreement. The LE Directive specifically refers to the ECHR and to the right to an effective remedy and to fair trial in Paragraph 104. The analysis of the SWIFT Agreement in chapter 3 of this study, however, has shown that the remedies that are ensured for within the agreement are inconsistent with EU

data protection standards since they are only available under US law. The possibility of problems regarding remedial powers due to inconsistent legal regimes in the context of data transfers to third states is even being acknowledged by the LE Directive (Paragraph 74). In addition to the provision of effective remedies, the LE Directive furthermore requires the provision of the right to compensation to any natural or legal person that has been damaged due to unlawful processing of his or her personal data. However, the SWIFT Agreement does not provide for any form of compensation. Since the US data protection framework precludes non-US persons from compensation as well, there is no legal provision for EU citizens to get access to this right of the LE Directive when their personal data is being processed in the context of the TFTP.

The protection of the EU citizen's fundamental right to data protection and the consistency of the SWIFT Agreement with the LE Directive is furthermore challenged by the the very fact that the SWIFT Agreement includes the transfer of personal data from the EU to the US. The LE Directive requires that personal data can only be transferred to a competent authority of a third country for specified, explicit and legitimate purpose and must either be based on an adequacy decision by the Commission or be based on appropriate safeguards. While the UST displays the competent authority in the US within the SWIFT Agreement and the purpose is also limited by the Agreement, neither the US nor SWIFT and the TFTP are part of an adequacy decision since the ECJ invalidated the safe harbour decision in its judgment on the case *Maximilian Schrems v Data Protection Commissioner* of 6 October 2015 (Schrems case). In the case, the ECJ found that Safe Harbour did not provide for an adequate protection of fundamental rights and freedoms guaranteed in the EU and declared the Safe Harbour Framework invalid. Regarding the possible partiality of the Commission within the joint reports of the SWIFT-II agreement it should be noted at this point that the Commission found that the framework of Safe Harbour ensured for an adequate protection of personal data within personal data transfers from the EU to the US. The judicial review by the ECJ in its judgment on the Schrems case, however, constitutes a different conclusion on the data protection standards within this framework.

The SWIFT Agreement could display the legally binding instrument that is required by the LE Directive to allow data transfers to third states in the case an adequacy decision is missing. It is debatable whether the agreement provides for appropriate safeguards when considering the missing administrative and judicial remedies under EU law, the missing right for compensation for EU citizens and the bulk data collection under the SWIFT Agreement.

The LE Directive, however, does not automatically presuppose that existing international agreements are being amended and aligned with the LE Directive.

On the opposite, the LE Directive holds that “International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that data shall remain in force until amended, replaced or revoked”. Therefore, it is not required that existing international agreements must be changed to comply with the LE Directive. Article 61 leaves open the possibility of amendment, replacement and revocation. Therefore, the LE Directive can not be said to properly protect EU citizens rights regarding the SWIFT Agreement and the combination of the LE Directive and the SWIFT Agreement do not provide for a consistent legal framework of data protection for EU citizens.

6. Conclusion

6.1 Summary of Core Findings and Answer to the RQ

The EU and the US data protection framework, the SWIFT Agreement and the LE Directive have been analysed to derive to conclusions about the extent to which the SWIFT Agreement protects personal data of EU citizens in accordance with EU data protection standards. It has been found that the data protection frameworks of the European Union and the United States differ in their nature, scope and extent to which they protect personal data. Overall, the EU data protection framework displays a more comprehensive framework that includes data protection rights for every person. The right to data protection in the EU is considered a fundamental right and is specifically protected within EU primary law in Articles 16 TFEU and Article 8 CFREU. The US regal framework on data protection, to the contrary, is much more fragmented. Unlike in the EU, there is no specific constitutional protection of personal data despite the Fourth Amendment which can be interpreted to include the right to privacy and data protection. Apart from that, only the Privacy Act of 1974 constitutes a legal measure aiming at a comprehensive protection of personal data. The rights of both the Fourth Amendment and the Privacy Act, however, are only granted to US persons, excluding EU citizens from their scope of applicability. Also, neither the Privacy Act nor the Fourth Amendment set any regulations on data collection via the US TFTP because the former permits data sharing for law enforcement purposes, and provisions of the latter do not apply because of the “third party doctrine”.

Only, the Judicial Redress Act and the Umbrella Agreement constitute slight improvements for the rights of EU citizens in the context of data sharing between the EU and the U.S, however, it is not sure whether the Judicial Redress Act and the Umbrella Agreement function effectively in their purposes. This is to be seen in future judgements of the ECJ who upholds the high standards of EU data protection. Even though the Commission states that the both the Umbrella Agreement and the SWIFT Agreement provide for adequate protection of EU citizens rights in the context of transatlantic data sharing, it has to be kept in mind that its adequacy decision on the Safe Harbour framework was invalidated by the ECJ.

Within the analysis of the SWIFT Agreement one can notice a tilt towards a US dominance and a dominance on security rather than privacy protection. While the SWIFT Agreement is consistent with the formal data protection rights and principles of the LE Directive and EU primary law terms of its processing of personal data and the transparency or its actions, challenges for the protection of EU citizen's personal data derive from problems regarding possibly ineffective administrative and judicial remedies and insufficient judicial review. Within the SWIFT Agreement it is not assured for effective remedies that comply with the high data protection standards ensured for in the EU data protection framework, since they are only available under the US data protection framework. The SWIFT Agreement shows a clear dominance of US law. This contrasts with the self-expression of the agreement in the preamble as an agreement of two equal partners and underscores the findings of Servent and MacKenzie (2012) that EU and EP continued to act as norm takers within the SWIFT-II Agreement.

The LE Directive could have promoted EU data protection standards within the transatlantic relationship and could have led to a change from the EU as a norm taker of US security norms to a norm maker of data protection norms. However, already the instrument of a Directive, which is weaker than a Regulation, raises doubts. While the GDPR is directly applicable in third states outside the European Union, the LE Directive is not even directly applicable within the European Union and must first be transposed into national law. Therefore, it is not given that the Directive does in fact reach its goal of a harmonised data protection in the realm of JHA within the European Union. This is highlighted by the fact that the LE Directive only applies to actions that fall within the scope of Union law. In the context of the SWIFT Agreement, this is especially important since neither Europol nor Eurojust are being addressed by the LE Directive. However, both agencies, Europol in particular, play an important role regarding the TFTP and can request data via the SWIFT Agreement. This limits the protection of personal data by the SWIFT Agreement and the LE Directive.

The choice of a Directive as the means highlights the continuing difficulties to harmonise legislation between EU member states within the realm of security, not only regarding data protection but also regarding a comprehensive refugee policy or counter-terrorism strategy. The protection of security is an issue that lies at the heart of EU member states sovereignty. In the past, it has also been EU member states – by means of the EU council – who promoted the outsourcing of security to the United States, if necessary, also to the disadvantage of data protection. Therefore, the EU has been acting as a norm taker in the transatlantic counter-terrorism strategy in the past. This did not change in the aftermath of the Lisbon Treaty which becomes obvious when looking at the unsatisfactory data protection within the SWIFT Agreement, the first agreement in which the EP had the chance to co-decide on the adoption of the agreement. The LE Directive does not lead to a change in this power relationship either. It is an instrument of much lower influence than the Lisbon Treaty has been and it leaves loopholes for the SWIFT Agreement to keep existing even though it is not consistent with substantial EU data protection standards. The SWIFT Agreement does not ensure for the enforcement of the fundamental right to data protection and the LE Directive enables Europol to access TFTP data without regulating its actions. The SWIFT Agreement is also not consistent with the LE Directive and EU data protection standards when it comes to control and review mechanisms in terms of independence. In the SWIFT Agreement, neither Europol in its pre-transfer control nor Commission and the UST within the joint review are free from bias as all three are in favour of the TFTP and the SWIFT Agreement. While the LE Directive is consistent with EU data protection standards, it once again displays that the protection of security and security cooperation between EU and US trumps the protection of privacy. However, by 6 May 2019 the Commission is asked to

> "*review other legal acts adopted by the Union which regulate the processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive*" (Article 62 (6)).

Despite the SWIFT Agreement's inconsistencies with the requirements of the LE Directive and the fact that it is not assured that the rights to data protection within the SWIFT Agreement are really made available to EU citizens at a standard of EU data protection

law, it is to be seen whether any changes or amendments will be made to the SWIFT Agreement following the Commission reviews. Since the Commissions review of the TFTP and the SWIFT Agreement continue to be positive, it can be assumed that the Commission will not find that the data processing within the SWIFT Agreement is not aligned with the LE Directive. For the time being, the SWIFT Agreement will remain valid despite the fact that its substantial data protection safeguards are not in accordance with EU data protection standards.

6.2 Implications and Outlook

The present analysis on the extent to which personal data of EU citizens is protected within the EU-US SWIFT Agreement adds to existing research within the area of transatlantic counter-terrorism cooperation, especially as it includes the newly introduced Law Enforcement Directive of the European Union. The analysis has revealed that the SWIFT Agreement does not provide for a protection of EU citizens that is in accordance with EU standards on data protection. Furthermore, the findings of this study agree with previous findings that the EU displays a norm taker within the transatlantic counter-terrorism cooperation. In evaluating the consistency of the SWIFT Agreement with both EU data protection standards of EU primary law and the so far most comprehensive Directive for the protection of personal data within the scope of the JHA, the extent of EU citizen's data protection within the SWIFT Agreement could be adequately analysed.

However, other studies should take into consideration further existing international agreements of the EU and the US which aim to protect personal data in the context of data transfers between the EU and the US, such as the EU-US Privacy Shield and the Umbrella Agreement. Also, the Judicial Redress Act should be considered more extensively to analyse how and to what extent it increases the data protection rights of EU citizens in the US. To include these agreements in detail within this research would have exceeded the scope of this study. Nevertheless, it is of interest to analyse if these agreements increase the protection of EU citizens personal data within the transatlantic counter-terrorism cooperation and in the context of the SWIFT Agreement in particular. Also, further research should take a closer look on the individual EU institutions and agencies, especially Europol and Eurojust, to see how the protection of personal data is ensured when these agencies are involved. Thereby, especially the limited scope of the LE Directive in this realm should be taken into consideration.

Furthermore, more empirical research and implementing studies will have to be conducted on the SWIFT Agreement and the LE Directive in order to substantiate the findings of this study. Especially research on future ECJ judgments and Commission reports in relation

to transatlantic data sharing agreements and the LE Directive and the SWIFT Agreement can be of great interest.

References

Articles

Amicelle, A. (2013). The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From criticism to imitation of dataveillance. *CEPD Paper in Liberty and Security in Europe*. Retrieved July 1, 2018, from http://aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf

Archick, K. (2016). U.S.-EU Cooperation Against Terrorism, *Congressional Research Service*

Bignami, F. (2015). The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens. *SSRN Electronic Journal*,1-35. doi:10.2139/ssrn.2705618

Boehm, F. (2015). A comparison between US and EU data protection legislation for law enforcement purposes. *Institute for Information, Telecommunication and Media Law, University of Münster, Germany*. Retrieved June 19, 2018, from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

Busser, E. D. (2010). EU data protection in transatlantic cooperation in criminal matters Will the EU be serving its citizens an American meal? *Utrecht Law Review*,6(1), 86. doi:10.18352/ulr.116

Coolsaet, R. (2010). EU counterterrorism strategy: Value added or chimera? *International Affairs*, 86(4), 857-873. doi:10.1111/j.1468-2346.2010.00916.x

Exten, S. E. (2006). Major Developments in Financial Privacy Law 2006: The SWIFT Database Incident, and Updates to the Gramm-Leach-Bliley and Fair Credit Reporting Acts. *Journal of Law and Policy for the Information Society*, 3(3), 650-676.

Keohane, D. (2007). The Absent Friend: EU Foreign Policy and Counter-Terrorism. JCMS: *Journal of Common Market Studies*, 46(1), 125-146. doi:10.1111/j.1468-5965.2007.00770.x

Matera, C. (2016). Writing a thesis or a research paper in law at university

Monar, J. (2015). The EU as an International Counter-terrorism Actor: Progress and Constraints. *Intelligence and National Security*, 30(2-3), 333-356. doi:10.1080/02684527.2014.988448

Pfisterer, V. (2010). The Second SWIFT Agreement Between the European Union and the United States of America – An Overview. *German Law Journal*, 11(10), 1173-1190.

Porter, A. L., & Bendiek, A. (2012). Counterterrorism cooperation in the transatlantic security community. *European Security*, 21(4), 497-517. doi:10.1080/09662839.2012.688811

Servent, A. R., & MacKenzie, A. (2012). The European Parliament as a 'Norm Taker'? EU-US Relations after the SWIFT Agreement. *European Foreign Affairs Review* 17, Special Issue (2012): 71-86. Kluwer Law International BV, The Netherlands

Solove, D. J. (2002). "Conceptualizing Privacy." *California Law Review*, 90(4), Retrieved July 2, 2018, from https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview

Westin, A. F. (2003). Social and Political Dimensions of Privacy. Journal of Social Issues, 59(2), 431-453

Whitman, J. Q. (2003). The Two Western Cultures of Privacy: Dignity versus Liberty. SSRN Electronic Journal. doi:10.2139/ssrn.476041

Books

Hert, Paul De, and Papakonstantinou, Vagelis (2018). Data Protection Policies in EU Justice and Home Affairs: A Multi-layered and Yet Unexplored Territory for Legal Research. The Routledge Handbook of Justice and Home Affairs Research, 169-79. New York.

Murphy, C. C. (2012). Part III: THE FUTURE OF EU COUNTER-TERRORISM. 8. Rule of Law and Pre-Emption Reconsidered. EU counter-terrorism law pre-emption and the rule of law. Oxford and Portland, Oregon: Hart

Rees, G. W. (2006). Transatlantic counter-terrorism cooperation the new imperative. Abingdon: Routledge.

Internet Sources

Beuth, P. (2016, January 29). Alles Wichtige zum NSA-Skandal. Welche Daten sammelt die NSA, was ist Prism und wie reagieren die Überwachten? Aktuelle Entwicklungen und ein Überblick über die Snowden-Enthüllungen seit Juni 2013. Die Zeit. Retrieved July 1, 2018, from https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal

Council of Europe. (n.d.). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved June 19, 2018, from

https://www.coe.int/en/web/impact-convention-human-rights/convention-for-the-protection-of-individuals-with-regard-to-automatic-processing-of-personal-data#/

Deutsche Bundesbank. (2017). Glossary. Retrieved from https://www.bundesbank.de/Navigation/EN/Service/Glossary/Functions/glossary.html?lv2=129548&lv3=163238

European Commission. (2015a). Special Eurobarometer 431 “Data protection” (pp. 1-220). DOI 10.2838/552336. Retrieved June 6, 2018, from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

European Commission (2015b). European Commission - Fact Sheet. Questions and Answers on the EU-US data protection "Umbrella agreement". Retrieved June 20, 2018, from http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

European Commission. (2018a). Types of EU law. Retrieved June 06, 2018, from https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

European Commission. (2018b). What is personal data? Retrieved July 2, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Commission (n.d.). What does the General Data Protection Regulation (GDPR) govern? (2018, March 14). Retrieved June 20, 2018, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

European Parliament. (2010). Parliament examines SWIFT II agreement. Retrieved July 1, 2018, from http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20100205BKG68527&language=EN

European Parliament. (2016). Europeans in 2016: Perceptions and expectations, fight against terrorism and radicalisation. Retrieved June 6, 2018, from http://www.europarl.europa.eu/atyourservice/en/20160623PVL00111/Europeans-in-2016-Perceptions-and-expectations-fight-against-terrorism-and-radicalisation

General Secretariat of the Council. (2017). Data protection reform. Retrieved June 30, 2018, from http://www.consilium.europa.eu/en/policies/data-protection-reform/

Glossary of Summaries. Schengen (Agreement and Convention). (n.d.). Retrieved June 30, 2018, from https://eur-lex.europa.eu/summary/glossary/schengen_agreement.html

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama. The Guardian. Retrieved

July 1, 2018, from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Judicial Redress Act of 2015. (n.d.). Retrieved June 20, 2018, from https://www.justice.gov/opcl/judicial-redress-act-2015

Laudati, L. (OLAF Data Protection Officer) (2016). Summaries of EU court decisions relating to data protection 2000-2015. Retrieved July 2, 2018, from https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf

Rechtslexikon.net. (n.d.a). Lex specialis derogat legi generali. Retrieved July 2, 2018, from http://www.rechtslexikon.net/d/lex-specialis-derogat-legi-generali/lex-specialis-derogat-legi-generali.htm

Rechtslexikon.net. (n.d.b). Lex superior derogat legi inferiori. Retrieved July 2, 2018, from http://www.rechtslexikon.net/d/lex-superior-derogat-legi-inferiori/lex-superior-derogat-legi-inferiori.htm

Rechtslexikon.net. (n.d.c). Lex posterior. Retrieved July 2, 2018, from http://www.rechtslexikon.net/d/lex-posterior/lex-posterior.htm

SWIFT FIN Traffic & Figures. (n.d.). Retrieved June 21, 2018, from https://www.swift.com/about-us/swift-fin-traffic-figures

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance (2013). Justice Information Sharing. Privacy Act of 1974, 5 U.S.C. § 552a. Retrieved June 20, 2018, from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279

U.S. Department of the Treasury (n.d.). Resource Center. Terrorism and Illicit Finance. Terrorist Finance Tracking Program. Retrieved July 1, 2018, from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx

Legislation and Policies

Article 29 Data Protection Working Party. (2014a). Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, adopted on 27 February 2014.

Article 29 Data Protection Working Party (2014b). Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive. Adopted on 1 August 2014. Retrieved July 1, 2018, from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf

Council of Europe (2010). European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13. Retrieved June 6, 2018, from https://www.echr.coe.int/Documents/Convention_ENG.pdf

Council of the European Union (2009). European Security Strategy – A secure Europe in a better world. DOI 10.2860/1402. Retrieved July 3, 2018 from https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf

European Council (2001). Conclusion and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001. Retrieved July 1, 2018, from https://www.consilium.europa.eu/media/20972/140en.pdf

European Council. (2004). EU-U.S. declaration on combating terrorism. Dromland castle, 26 June 2004. 10760/04 (Presse 205)

European Parliament (2007). European Parliament resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues. Retrieved June 21, 2018 from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0039+0+DOC+XML+V0//EN

European Parliament (2013). European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance. Retrieved June 27, 2018 from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0449&language=EN

European Parliament (2014). European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. Retrieved June 27, 2018 from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230

European Parliament (2015). European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens. Retrived June 27, 2018 from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//EN

European Parliament and Council of the European Union (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available

electronic communications services or of public communications networks and amending Directive 2002/58/EC.OJ L105

European Parliament and Council of the European Union (2016a). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. O.J. L119

European Parliament and Council of the European Union (2016b). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). O.J. L 119

European Union. (2012a). Charter of Fundamental Rights of the European Union. OJ 2012/C 326/2 (Vol. 55, p. 391). Retrieved June 19, 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2012:326:TOC

European Union (2012b). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Consolidated version of the Treaty on European Union. OJ 2012/C 326/1 (Vol. 55, p. 13). Retrieved June 19, 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2012:326:TOC

European Union (2012c). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Consolidated Version of the Treaty on the Functioning of the European Union. OJ 2012/C 326/1 (Vol. 55, p. 47-201). Retrieved June 19, 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2012:326:TOC

European Union (2012d). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007. OJ 2012/C 326/1 (Vol. 55, p. 337-391). Retrieved June 30, 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2012:326:TOC

European Union & United States of America. (2010). Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program. O.J. L 008 , 13/01/2010 P. 0011 - 0016

European Union & Unites States of America (2015). Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses.

UN General Assembly. (1948). Universal declaration of human rights (217 [III] A). Paris. Retrieved June 19, 2018 from http://www.un.org/en/universal-declaration-human-rights/

U.S. Constitution (1791), amend. IV.

Television

Reding, V. (Interviewee) (2018, Mai 15). Werbung – Das Geschäftsmodell von Facebook. In R. Yogeshwar (presenter). Quarks & Co. Germany: Westdeutscher Rundfunk (WDR)