University of Twente
Faculty of Behavioral, Management and Social Science
Public Governance across Borders

Marie Middelstorb
s1819429

Bachelor Thesis

"The European Union's balancing between security objectives and data protection.
The case of Passenger Name Record data"

First Supervisor: Dr. Claudio Matera
Second Supervisor: Dr. Pieter-Jan Klok

04th of July 2018

ABSTRACT

Facing confrontation with a new dimension of security threats resulting from the rise of terrorism and serious organized crime, police and security authorities aspire to intensify international cooperation. Adjusted collaboration practices involve enhanced exchange of data across borders, which is a practice causing legal concerns regarding data accessibility and protection. This research aims to investigate the consistency between external data transfers for the purpose of fighting terrorism and serious crime and data protection obligations stated in the European legal framework. Since arising discrepancies between internal and external data safeguards are theoretically possible when data is proceeded to third countries, the research further intends to draw conclusions on how the European Union balances these against the pursuit of strategic security objectives. In other words, the European relationship between security targets on the one hand and data protection obligations on the other shall be outlined. Accordingly, the main research question studies the extent to which European data protection standards enable information exchange in the fight against terrorism and serious crime whilst safeguarding personal data of European citizens. Grounded within legal research, the study is composed of a qualitative, conceptual research design, that follows explanatory, hermeneutic but also evaluative approaches. It is based on a case study design stressing controversial transfers of Passenger Name Record (PNR) data. To enter the PNR case and to answer the research question, information is retrieved from contemporary policy and regulatory frameworks, in case law and literary analysis by legal researchers.

TABLE OF CONTENT

LIST OF ABBREVATIONS

AFSJ	Area of Freedom, Security and Justice
API	Advanced Passenger Information
CFREU	Charta of Fundamental Rights of the European Union
CFSP	Common Foreign and Security Policy
CJEU	European Court of Justice
EU	European Union
ECHR	European Convention of Human Rights
ECTC	European Counter Terrorism Centre
ECtHR	European Court of Human Rights
EEA	European Economic Area
ENTER	European Network of Experts on Radicalization
ICT	Information and Communication Technology
IDPC	Irish Data Protection Commissioner
ISS	Internal Security Strategy
JHA	Justice and Home Affairs Council
MEP	Member of the European Parliament
MOU	Memorandum of Understanding
NGO	Non-governmental Organization
PIU	Passenger Information Unit
PNR	Passenger Name Record
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
US	United States

1. INTRODUCTION

"In the face of a multiform terrorist threat directly targeted against our values, we reaffirm our unfailing solidarity and our determination to fight together against terrorism […] in accordance with human rights and fundamental freedoms." (Council of Ministers, 2015). This statement was issued jointly after the crisis meeting of the interior ministers in light of the terrorist attacks in Paris in 2015. It stresses the new European security agenda resulting from the increased terrorist threat in Europe, marking a turning point on Europe's Internal Security Strategy (ISS). Simultaneously, it demonstrates the European commitment to the protection of fundamental human rights according to values and principles emerging from key legal frameworks, for instance from Article 8.2 of the European Convention for the Protection of Human Rights and Freedom (ECHR, 1950).

However, the envisaged interests are partly conflictual, despite both having legitimation (Asinari & Poullet, 2004). In the past decade, legal challenges on the security of European citizens' data emerged from the rise of technological development. In the digital age, advanced IT systems daily collect an extensive number of individuals' private data. This creates supplementary opportunities for public authorities to face terrorist and criminal threats, including integrated cross-border information sharing between national security departments. Thus, data that was gathered by one country, is processed and retained by different nations' security authorities. The practice extends the opportunistic scope of law enforcement authorities, but simultaneously increases the risk for creating an Orwellian society characterized by mass-surveillance and bulk data traffic. Public awareness on this has been raised in recent years resulting in more concerns about the accessibility of individual's personal data (ICO, 2015).

To keep up with the altered settings of a data-driven society, the European Union (EU) introduced a revised set of secondary law in 2016, which redefines the European legal framework on the processing of personal data. The reform package is officially promoted as "an essential step to strengthening citizens' fundamental rights in the digital age" (Commission, 2017a). A significant amount of data from European citizens is, however, not only shared across Member States but transferred to third countries, whose legal standards of data protection may differ considerably from European safeguards. To illustrate how such cross-border data sharing with third countries for public security purposes is consistent with data safeguards emerging from the European regulatory framework, the specific case of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime will be investigated in detail. To analyze the scope of PNR data transfers in a comprehensive manner within the case study, the EU internal and external dimensions of such data proceedings are addressed separately.

1.1. Research Questions and Methodology

The study aims to provide a contribution to the discussion about the level of protection of EU citizen's personal data in third countries. Does the data maintain its level of protection when being transferred to Non-European countries or do data transfers entail shortcomings of this standard? What does the answer imply for the European approach on counter-terrorism and crime detection? To approach these questions, the study scrutinizes the balance between adequate protection of personal data, including maintenance of protection standards when data is proceeded across EU-borders and security objectives. This is done based on an evaluation of the consistency between external data transfers for security purposes and intra-European standards on privacy and data protection. Thereby, the research follows a top-down approach, starting with the examination of strategic rationales of data utilization in the field of law enforcement, before shifting emphasis to PNR data proceedings within a case study design. PNR data is increasingly central to the debate about safeguards for external data proceedings, especially since the European Court of Justice (CJEU) issued Opinion 1/15 on the draft agreement for PNR data transfers between the European Union and Canada. Based on the findings from the case-study, the consistency between external data transfers and internal protection standards is assessed before a conclusion on the delicate balance between both rationales is drawn.

1.1.1. Main Research Question and Subquestions

The study is based on the main research question (RQ):

RQ: *To what extent do European data protection standards enable external data proceedings in the fight against terrorism and serious crime whilst safeguarding personal data of European citizens?*

The main research question incorporates characteristics of an explanatory and hermeneutic question (Matera, 2016). It aims to outline the relationship between public security and personal data protection in examining the balance between these two in the context of international PNR data transfers. For this purpose, the study examines the extent to which provisions on privacy and data protection allow the EU and its Member States to share personal information with third countries in the law enforcement sector. Four subquestions (SQ) were identified to frame a consistent answer to the main research question.

SQ1: *Which protection standards apply on the processing of personal data in the European security environment and how do they affect counter-terrorism cooperation with third countries?*

The first subquestion is composed of explanatory and logical characteristics (Matera, 2016). It provides knowledge on the legal background applicable for data proceeding methods in the law enforcement field and, hence, forms the foundation for the subsequent research. Moreover, it engages the practical effects

of data processing legacy on bilateral counter-terrorism cooperation between European and third country's security authorities.

Firstly, the subquestion shall demonstrate the humanitarian basis of data protection through the investigation of universal principles, that are embedded in fundamental rights (*section 2.2*). To enhance the human rights perspective, implications emerging from international law, for instance Article 8 ECHR, are scrutinized. Thereafter, the European legislative framework on the protection of personal data is tackled (*section 2.3*). EU legislation on the protection of personal data is tackled more broadly before the focus is shifted to specific laws on data protection in the police and justice sector. In this context special emphasis lies on Directive 2016/680. As cross-border data proceedings largely fall within the scope of security cooperation, the character of the European law enforcement strategy is discussed subsequently.

Secondly, for the introduction of the practical dimension, the subquestion targets the analysis of implications emerging from EU protection obligations on data transfers in the sphere of counter-terrorism cooperation between the European and international judicial bodies (s*ection 2.4*). In this aspect, the relationship between the EU and the United States (US) deserves special attention. The fundamental differences between the countries approaches on data protection illustrate how European core values clash with external partner's viewpoints despite sharing the common goal of ensuring security. Besides, relationship is traditionally close and impacts the European security cooperation with other countries considerably (Argomaniz, 2009).

SQ2: *What is the existing regulatory framework on PNR data within the EU and does it provide sufficient protection safeguards?*

The second subquestion combines attributes of explanatory research with a hermeneutic approach (Matera, 2016). Emphasizing three significant aspects of PNR data jurisdiction is an essential element of this chapter which aims to introduce the status of PNR data legislation within the EU. The aspects include general knowledge about PNR data (I), the current regulatory framework as part of the data protection reform package (II) and the sufficiency of data protection safeguards inhabitant in European PNR legislation (III).

To tackle the subquestion, the relevance, background and utilization of PNR data are approached for making an explanatory starting point in the introduction (*section 3.1*). This includes, *inter alia*, further links on how the data is embedded in the European security strategy and how the share of bulk mobility data improves counter-terrorism operations throughout the Member States. Providing a comprehensive overview on internal PNR policy, Directive (EU) 2016/681 as the current regulatory framework is illustrated (*section 3.2*). Thereby, legal instructions that have been imposed in CJEU case-law shall be

analyzed considering the main reasons underlying such modifications. Afterwards, the chapter outlines reservations on the sufficiency of data protection safeguards as embedded in Directive (EU) 2016/681 (*section 3.3*).

SQ3: *Which principles for international data transfers emerge from PNR agreements between the EU and third countries?*

Following the character of an explanatory, hermeneutic and logical typology (Matera, 2016), the third subquestion introduces the external dimension of PNR data. As a starting point, the development of bilateral PNR agreements concluded between the EU and third countries is presented by scrutinizing the main factors that have led to changes in the agreement's history (*section 4.2*). To explain the dominant data protection principles shaping the processing of PNR data from a juridical point of view, the current bilateral agreements between the EU and third countries are then analyzed *(section 4.3*). The key interest here lies in the factual level of data protection provided for in the bilateral agreements. A methodological framework categorizes the main elements of the PNR agreements, such as provisions on the data retention period, in order to structure the analysis in a comprehensive manner. The framework allows the chapter to compare the agreements directly as well as to detect non-evident restrictions on fundamental rights that may arise from legal derogations.

SQ4: *To what extent are external PNR data transfers for security purposes consistent with European data protection standards?*

The final subquestion conflates the knowledge from the former questions by linking internal EU data protection and privacy standards to external PNR data proceedings with third countries. It explicitly combines the findings on data protection safeguards in the law enforcement sector as conditioned within the European legal system (subquestion 1-2) with exchange practice determined by the third-country PNR data transfer agreements (subquestion 3). In addition, the subquestion provides the final element for scrutinizing consistency on a comprehensive basis by evaluating implications on external data proceedings emerging from two crucial landmark decisions by CJEU. In other words, it aims to assess the extent to which intra-European PNR data regulations are consistent with legal safeguards of third countries receiving PNR data from European authorities. Given this, it unites characteristics of evaluative, explanatory and hermeneutic types of legal research (Matera, 2016). The argumentations of interest given by the CJEU relate to the Schrems case and Opinion 1/15. Because the subquestion's emphasis is put on PNR data, it builds on the findings of the Opinion and outlines implications on security-related data flows outside of the EU (*section 5.2*). Thereby, legal challenges on the right to data protection are addressed, which finally enables the subquestion to tackle the question of consistency and

to answer whether PNR data flows outside of the EU respect data protection standards emerging from the Treaties and the CFREU. This step represents the evaluative manner of the question.

In the subsequent chapter an answer the main research question is concluded. Based on the findings of the former chapters, it reveals if EU standards on the protection of personal data constitute an obstacle for the proceeding of data to third country's security and police authorities.

1.1.2. Methodology and Body of Knowledge

Following a systematic approach, the study examines the extent to which personal data retains its level of protection provided for by EU law, when it is being proceeded to third country's security authorities. Such external information proceedings disclose crucial areas of tension since legal frameworks in terms of privacy regulations and safeguards in data-receiving third countries may differ considerably from strict standards prevalent in the EU. Given these discrepancies, personal data may loose its protection standard guaranteed within the EU once it is proceeded externally. Although the EU tends to attach importance to the compliance of third countries with foreign data protection standards, the assessment is influenced by the pursuit of security objectives, including the prevention of terrorist threats and serious criminal offenses. Given this, this study shall evaluate how objectives emerging from European ISS are proportionate to compliance with data protection provisions. This reflects the balance between two conflicting leitmotivs, public security and data protection. Balance in its meaning does in this case not refer to trade-offs between the motives. Rather it is about the EU establishing an equilibrium to the forces of security and data protection, which combines the challenges within the relationship the best way possible. This is essentially done through a careful regulation of different policies which in the end shall reconcile the powers in line with the European rule of law. By examining external PNR data proceedings for law enforcement purposes, the study aims to clarify how the progress of finding an equilibrium between security and data protection may proceed. In recent years, PNR data proceedings have become an increasingly popular measure in the fight against terrorism and serious crime because it allows police authorities to monitor air travel on the grounds of big data. Critical voices are however concerned about bulk collection of non-suspect's reference and long retention periods emerging from the practice. Given such reservations, the legislative grounds of PNR data utilization were recently challenged in front of the CJEU. This assigns the matter with great relevance and allows further reflections on the future course of reconciling security and privacy interests in light of the study's main research question.

Throughout the study, an answer to the main research question is developed based on four subquestions. These do not only combine explanatory and hermeneutic characteristics but also touch upon logic and evaluative research approaches as well. Each subquestion stresses certain aspects with relevance for the conclusion of the main research question. These aspects are analyzed based on the interpretation of application and development of regulatory frameworks, case law and legal principles of the EU.

Information is gathered from a set of different origins including European primary and secondary law, policy papers, case law and independent analysis by legal researchers. Since the study is classified within the field of legal research, a qualitative, conceptual research design is key to conclude an answer to the main research question. The relationship between public security and the protection of individual's private data within the EU is primarily addressed in the first subquestion, whereas the case-study on PNR data is embarked in the second and third subquestion. Thereby, the EU internal dimension of PNR data is emphasized in the second subquestion and the external dimension in the third subquestion. The fourth subquestion is designed to draw inference on PNR data practice based on the combination of findings derived from the former subquestions. This enables the question to conclude if discrepancies between internal and external data safeguards exist, or in other words, if PNR data transfers for security purposes are consistent with EU privacy and data protection standards. For answering the main research question in the end, the outcome of the fourth subquestion in terms of consistency is crucial. In case discrepancies on protection safeguards occur when PNR data is transferred externally, the evaluation of the EU's balancing between security objectives and data protection regulations is different to when no inconsistencies transpire. Given the event that European standards on data protection are not fully applied on data proceedings to third countries, the study will reflect on the question whether they can be considered an obstacle to security cooperation. However, if external PNR data transfers are fully consistent with European data protection standards, legal instruments for maintaining the status in the future shall be outlined in the conclusion. In any case, to ensure that a comprehensive picture is provided, policy recommendations for future legal frameworks on PNR data usage for security aims are presented.

1.2. Key Concepts and Theory

The main research question entails security and privacy as central analytical concepts, which are presented and discussed in the following. Given the need of the EU to reconcile security objectives and fundamental rights, whilst respecting ethical provisions and conformity with the law, the significance that derives from the balance of both concepts, security and privacy, becomes evident. The subject is not only characterized by high complexity, but also demonstrates great sensitivity arising from public reservations on the proceeding of PNR data. In the following security and privacy shall be subject of conceptualization and theoretical review. The terms outlined in relation to security are: European internal security and defense strategy, counter-terrorism and serious crime and PNR data. In relation to privacy, the section clarifies: Human rights, right to privacy and data protection.

1.2.3. European Internal Security and Defense Strategy

The scope of all strategic actions is based on the legal provisions stated in the Treaty on the European Union (TEU) and Treaty on the Functioning of the European Union (TFEU). The competences to adopt measures within the area of security and defense are divided between supranational governance in the Area of Freedom, Security and Justice (AFSJ), stipulated in the Treaty on the Functioning of the

European Union and intergovernmental structures prevalent in the Common Foreign and Security Policy (CFSP).

The AFSJ includes several policy domains, for instance, in the field of border policies, counter-terrorism and police and justice cooperation. This diversity in policy fields emerged from the extensive institutional development the AFSJ has undergone and results in an extremely broad and heterogenous scope as Kaunert et al. (2014) note. It shall ensure a maximum of security across all Member States in times of increasing vulnerability of core European values that is a result of rising threats of terrorism and crime. The recent terrorist attacks throughout Europe have brutally demonstrated this vulnerability and reopened discussions about security strategies. Thus, the EU ISS, which poses the latest formulation of strategy in the AFSJ field, aims to set out a common security model throughout the EU. It is composed of legislation and operational measures intended for responding to severe criminal actions. The security model promoted is characterized by strong "commitment to a mutually reinforcing relationship between security, freedom and privacy, and based on prevention, cooperation and solidarity between Member States […] and greater interdependence between internal and external security." (European Parliament, 2015a). The ISS does further stress the significant role of comprehensive, innovative and flexible measures with regards to the protection of European citizens. The key instrument for organizing an effective protection is however cross-border cooperation in terms of law enforcement, border management and civil protection. Cooperation efforts have always been particularly relevant for responding to criminal threats on the European level, especially in order to tackle security gaps deriving from free movement within the Schengen area (Wittendrop, 2016).

1.2.4. Counter-terrorism and Serious Crime

The European security environment has undergone extensive changes since 9/11. Prior to the attacks, the work of the Justice and Home Affairs Council (JHA) was mainly dominated by tackling organized crime, including for instance the trafficking of drugs or human beings. Terrorist threats were recognized, but not addressed within respective JHA action plans. In the aftermath of the 9/11 events, the long-term acceleration of European capacities to develop a cohesive and unified political-military power were addressed extensively (Golino, 2002). Correspondingly, the EU has identified the terrorist threat as one of the most pressing challenges and participates as an active player in countering it. As a matter of fact, some scholars declare contemporary terrorism as the most important of various key threats to the EU (Chirlesan, 2015; Dumitriu, 2004). Potemkina (2017) argues, however, that despite increased efforts taken with regards to European counter-terrorism measures, the diverging priorities prevalent within the European institutional framework result in biased implementation of anti-terror policies. Whilst the European Parliament and the public opinion have a rather critical stance towards additional rights restrictions for security purposes, the Commission follows a more liberal approach in the field. Potemkina's argument corresponds with Leonard's (2010) view, who notes that only a limited number of European counter-terrorism initiatives has made substantial contribution to the fight against terrorism.

Because no universal definition for terrorism exists, it is dependent on the researcher what to include in the concept. According to the North Atlantic Treaty Organization (NATO) terrorism is defined as "[t]he unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objective" (NATO, 2014). At the European level, Article 1 of framework decision 2002/475/JHA defines terrorist offenses in aftermath of the 9/11 attacks "as a combination of: objective elements (murder, bodily injuries, hostage taking, extortion, committing attacks, threat to commit any of the above, etc.); and subjective elements (acts committed with the objective of seriously intimidating a population, destabilising or destroying structures of a country or international organisation or making a government abstain from performing actions)." (Council, 2002).

In 2005 the EU counter-terrorism strategy stated four pillars for the fight against terrorism. These pillars target a strategy consisting of prevention, protection, pursuit and response (Council, 2005). The second pillar, protection, intents to ensure security not only for individuals but also for infrastructure. It includes improvements on transport security, which links it to the utilization of PNR data in aviation. Moreover, the EU counter-terrorism strategy fosters global engagement between public authorities, for instance, in terms of intensified dialogue and capacity-building. The list of measures enhancing cooperation efforts is correspondent with the ISS. The most relevant actors in managing internal and external anti-terrorism measures include, amongst others, the European Network of Experts on Radicalization (ENER), the European Defense Agency and Europol. The latter has established the European Counter Terrorism Centre (ECTC) in 2016, improving the organization of international cooperation among several counter-terrorism authorities and boosting European engagement in the global fight against terrorism.

1.2.5. Passenger Name Record Data

Cooperation in the security environment is required to address unwanted cross-border mobility of terrorist adequately to ensure a maximum level of public security. One suitable tool to encounter the issue and prevent security gaps is the utilization of PNR data for law enforcement purposes. PNR data includes a total of 34 areas of data, *inter alia*, information about contact details, means of payment, travel dates and itinerary and required when purchasing an airline ticket regardless of the tendering airline. PNR data developed in American security authorities resulting from internal restructuring operations after the 9/11 attacks (Balzacq, 2008). In the Schengen area, the data is crucial for counterbalancing the international organization of terrorism and severe criminal threats, that tend to benefit from abolished border controls. Regarding the processing of PNR data, the Council highlights the improved measures in law enforcement for the identification of suspects, investigations and prosecutions. International security authorities can, with the aid of predefined risk criteria, use PNR data to detect "persons unsuspected of crime or terrorism before a specific data analysis would show they might be." (Council, 2017).

1.3. Human Rights and Right to Privacy

As codified in Article 2 TEU, the European Member States are subject to legal obligations deriving from various international human rights frameworks. The most prominent of theses treaties is the United Nations' Universal Declaration of Human Rights (UDHR). Published long before the digital age, it emphasized special protection for the privacy and family life of individuals in 1948:

> Article 12
> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. (UDHR, 1948).

Article 12 carries considerable weight regarding modern legislation on privacy and can be viewed as the leading legal framework. The obligations stated in Article 12 ensure the protection of an individual's privacy from external intrusion of other individuals or the state. The right to privacy thereby safeguards key democratic values including human dignity, autonomy and freedom of speech (Privacy International, n.d.). In 1950, the European Convention of Human Rights (ECHR) adopted the principles applicable for the protection of privacy:

> Article 8 - Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (ECHR, 1950).

Throughout past jurisprudence the European Court of Human Rights (ECtHR) has clarified that states are not only obligated to prevent the violation of principles emerging from Article 8, but that they are also required to actively ensure respect for private and family life. However, despite being considered as a fundamental human right, the right to privacy is not absolute, which makes it subject to balance against other rights or interests under certain circumstances.

Within the European Union, Article 7 of the Charta of Fundamental Rights of the European Union (CFREU) serves as the legal basis for the protection of privacy:

> Article 7 – Respect for private and family life
> Everyone has the right to respect for his or her private and family life, home and communications. (CFREU, 2000).

Yet, the right to privacy is viewed as "one of the most important human rights issues of the modern age." (Privacy International, n. n.). This is mainly because of rising legal uncertainties and privacy concerns regarding the full compliance of information sharing on the internet with the right to privacy as defined in international law. Besides, enhanced mass surveillance and data analyzation practices by governmental authorities have triggered questions of legitimacy and respect to the rule of law in terms of privacy. For this study the reference to security threats made by many European security authorities to justify intensified surveillance powers is key, because of its suitability to PNR data collection and proceeding.

1.4. Data Protection

Data protection is closely intertwined with the right to privacy. Primarily, it prevents data from being lost or misused by public or private entities (Blasi-Casagran, 2017). The CFREU provides the following definition for the protection of personal data:

> Article 8 – Protection of Personal Data
> 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. (CFREU, 2000).

With view to the European treaties, data protection rights are guaranteed under Article 16 of the Treaty on the Functioning of the European Union:

> Article 16 (ex Article 286 TEC)
> 1. Everyone has the right to the protection of personal data concerning them. (TFEU, 2012).

The terminology "personal data", stated in Article 16.1 TFEU, is subject to precise definition in Article 4 of Regulation (EU) 2016/679, also referred to as General Data Protection Regulation (GDPR). Accordingly, personal data is any information relating to an identified or identifiable natural person,

also referred to as data subject. Reconsidering the scope of PNR data in light of this study, it becomes apprehend that the data protection provisions stated in the GDPR are applicable for PNR data. Besides personal data, so-called sensitive data is differentiated in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108). It concerns data on an individual's race, politics, health, religion, sexual life or criminal record, which requires enhanced protection and is therefore subject to a specified legal regime. Information gathered under PNR can easily be conflated so that conclusions may be drawn on individual's sensitive data (EDRi et al., 2015). Addressing the concept is, therefore, crucial to foster a comprehensive understanding for critical views on handling PNR data within the study.

The purpose of this research is to investigate the interconnectedness between the concepts related to security and privacy as outlined above. It addresses how security practices utilized by public authorities provide room for clashes with obligations on privacy and data protection. The case of PNR data in countering security threats illustrates the European predicament in a comprehensive manner. It is eligible for identifying precisely where security objectives may come into conflict with provisions deriving from the European legal and regulatory framework on data protection.

1.5. Social and Scientific Relevance

Considering that the relevance of data flows within the security environment has been outlined previously, this section intents to highlight the significance of PNR data. With the revised set of regulations on the protection of data that entered into force in May 2018, the EU adopts primary law on PNR data for the first time after failed attempts in 2011. For many years, security experts have argued in form of the harmonization of Member States' national provisions regarding the proceeding and retention of PNR data. Directive (EU) 2016/681 finally establishes a legal basis for the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime. It adopts mechanisms that support public authorities in countering the threat posed by terrorists and their increased mobility. This step effectively results from the terrorist attacks in Europe in the past years. Furthermore, PNR data regained broad attention in 2017 after the CJEU declared the negotiated PNR data transfer agreement between the EU and Canada invalidated. The judgment does not only affect the envisaged agreement but has further implications on the existing agreements with the US and Australia, future negotiations on additional PNR agreements and to some extent even on the PNR Directive. All in all, the EU will be required to reconsider its current approach on PNR data according to the evaluation of the CJEU. Any policy adaptions will in this context foster changes to the balance between the two main objectives, security and data protection. Due to the altered conditions, former research in the field of PNR data requires revision that includes contemporary perspectives on the subject.

2. DATA PROTECTION AND DATA FLOWS IN THE FIGHT AGAINST TRANSNATIONAL CRIME AND TERRORISM

2.1. Introduction to Data Protection and Data Flows in the Fight against Transnational Crime and Terrorism

After having approached the study's background in the introductory chapter, this chapter targets on concluding an answer to the first subquestion: Which protection standards apply on the processing of personal data in the European security environment and how do they affect counter-terrorism cooperation with third countries? The question outlines the European legal background on data protection by emphasizing the protection of personal data that is being transferred between judicial bodies in the fight against transnational crime and terrorism. In addition, it stresses practical implications on security cooperation between the EU and third countries resulting from European privacy obligations. As a starting point, the first section of this chapter introduces into the foundations of data protection (*section 2.2*). Thereby, reference is made to the legal framework stated in human rights law, which has been utilized previously for the definition of privacy and data protection. The subsequent section then gives a general overview on the European legislative framework on internal data protection obligations, including special regulations applicable in the police and justice sector (*section 2.3*). Additionally, the European law enforcement approach on countering the terrorism threat is analyzed. On that basis, the practical dimension of data protection within the security environment is pointed out afterwards (*section 2.4*). Finally, a conclusion to the first subquestion is formulated in the last section by considering the findings on existing internal EU data protection standards as well as on counter-terrorism approaches and reflect on their effects with regards to cooperation with third states' security authorities (*section 2.5*). The findings will benchmark the rest of the study as they approach not only PNR data but also general information exchange practice between security authorities. This is crucial for testing the consistency between external data transfers for security purposes and intra-European data protection regulations and thus for concluding an answer to the main research question.

2.2. Data Protection and Fundamental Rights

When converging data protection with regards to the concept's embeddedness in fundamental rights, privacy must be approached additionally in the interest of completeness. Being closely affiliated, both rights are aiming to preserve related human rights and freedoms, for instance the right to free speech or the freedom of religion. There are however some distinguishing aspects, that require further discussion. Privacy, in the notion of human rights, refers to the protection of a third actor's inference or attack on the individual's personal sphere. Stated in Article 12 UDHR, privacy is internationally recognized as a fundamental, human right. Consequently, most nations have incorporated the protection of "private life" from external interference in their national constitution. Unlike privacy, data protection is not accepted as a universal right amongst the international community. It evolves from the right to privacy but is more specific in its scope since referring to the online sphere primarily. Within this scope, it includes

any personal information to be found on the internet, that relate to a natural person directly or indirectly. Besides contact details or image and video material, the protection also comprises technical information such as the respective IP address. Importantly, an adequate level of protection entails fair collection, use and storage of personal information, but does not generally prevent such measures. This is because data protection, as well as privacy, are not absolute rights. Consequently, their scope of application is subject to legislative and judicatory interpretation. In confrontation with other EU key values, human and fundamental rights and public or private interests, a balancing against data protection and privacy may be possible. Thus, in presence of special circumstances, such as security concerns, restrictions on data safeguards may be established in in favor of conceding counterbalancing measurers to guarantee public security.

Within the European Union, limitations may be imposed only through legal acts implementing Article 16 TFEU and in respect of the CFREU. In non-EU countries, the respective interpretation within the legal system is, however, crucial in determining the national standards of data protection. As this interpretation differs considerably amongst the international community, the extent to which data is effectively protected is highly variable. Traditionally, governments are balancing interests in favor of either civil rights and liberties, privacy in this case, or security objectives. Depending on the key elements determined in the government strategy, one of the goals is either prioritized. Moreover, the extent to which each subjective is pursued is often subject to cultural preconditions. Evidence on this is most prominently preserved by the different privacy approaches held by the US and the EU. In the past, the transatlantic relationship has respectively been fraught with conflicts resulting from emerging disparities in the legal regimes. Case law, for instance in the aftermath of the Snowden revelations, has provided further evidence that the US tend to adjudge in favor of national privacy whereas the EU demonstrates a more accommodating position on unrestricted compliance with privacy and data protection (Dimitrova & Brkan, 2018).

In the EU, data protection has evolved from being a rather economic concept to a human right in the past decades (FRA, 2010). Especially due to altered technological conditions in the digital age, the issue has been placed on top of the political agenda. Having held high standards on data protection before, the EU lives up to its pioneering role in the field by establishing a clear commitment to the right to data protection in the modernized set of data protection legislation, which have entered into force in May 2018. While the provisions of Directive 95/46/EC were not yet framed in relation to the individual's right to data protection, the revised EU policy on data protection, the General Data Protection Regulation initially states:

> Article 1 – Subject matter and objectives
>
> This Regulation lays down rules relating to the protection of natural persons with

> regard to the processing of personal data and rules relating to the free movement of personal data. (GDPR, 2016).

The overall legal basis for the application of European data protection legacy is enshrined in Article 8 CFREU and Article 16 TFEU. Member States are legally bound to ensure the fundamental right to adequate protection of personal data according to the obligations emerging from the frameworks. In contrast to most human rights frameworks, the CFREU incorporates a division between privacy and data protection that was recognized in 2000 following a recommendation by the Article 29 Data Protection Working Party (Article 29 Working Party, 1999). The stand-alone right of data protection stated in the framework emerges from a set of factors, listed in Article 8 CFREU. Accordingly, the proceeding is required to be fair and to have a specific purpose on the consent of the person concerned or another legitimate basis laid down in the law. Additionally, the access and rectification must be ensured as well as control measures by an independent authority. Regardless of the context and domain (public or private sector), the individual is guaranteed the right of full control over his or her personal data.

On the basis of these provisions, the following principles can be identified for the protection of personal data in the EU (McDermott, 2017). The first principle, autonomy, is determined in relation to the right to full control over one's personal data. It targets to safeguard self-identity and human dignity by ensuring free and independent data handling for European citizens. Secondly, the principle of transparency stresses a rather practical dimension. Individuals are entitled to be informed about the nature and extent of data collection, utilization and consultation (EDPS, n.d.). Moreover, details regarding the processing of personal data must be openly accessible, clear to understand and retractable for the data subject. Finally, the principle of non-discrimination aims on excluding the effects of race, ethnicity, nationality, religion or sexual orientation from the processing of data, although providing legal space for profiling. In the CJEU judgment in Case C-524/06, the significance of the principle was confirmed by the highest legal authority the EU (Huber v Federal Republic of Germany, 2008).

Irrespective of the specific context, the detected principles apply on the absolute number of data proceedings in the EU. They have universal validity provided that the transfer is conducted within the EU internal dimension. As the study, however, aims to analyze the consistency of data transfers from the EU to third countries with data protection obligations emerging from the European legal framework, it extends the scope of data proceedings. When it comes to the introduction of the external dimension of data transfers, it may therefore be that the principles discussed with regards to the EU may not entirely comply to the essence of data protection in third countries. This must be noted for the further progress of the study.

2.3. European Legislative Framework

After having outlined the humanitarian basis of privacy and data protection, the EU legislative framework on data protection and data transfers shall be addressed in detail in the next section. Analyzing the specific provisions according to the contemporary European regulatory framework facilitates further elaboration on the protection standards for data proceedings and how they have evolved. Firstly, section 2.3.1 studies EU policies on data protection in a broader sense to provide a coherent basis of knowledge, before the focus is brought on data protection legislation applicant in law enforcement (*section 2.3.2*). Since the adoption of the new data protection package, Directive 2016/680 on Data Protection in the Police and Justice Sector serves as the legal foundation in the field. Therefore, the Directive will be the exclusive subject of interest in the section.

Moreover, by taking the security dimension of the study into consideration, emphasis is put on the character of EU counter-terrorism cooperation and strategy approaches. The section hence highlights the specific features and challenges prevalent in the field of law enforcement. In the past years, the EU has steadily adjusted the community law to encounter the altered conditions resulting from the effects of digitization. Especially the transformation process into a data-driven society has caused legal uncertainties and increased tensions between national security concerns and the respect to full protection of personal data. The strain on the relationship is primarily illustrated by security authority's extension of surveillance practices on Information and Communication Technologies (ICT). This, in combination with enhanced cooperative partnerships, constitutes the main alignment of the contemporary European counter-terrorism strategy, which is emphasized in section 2.3.3.

2.3.1. Legislation on the Protection of Personal Data

When approaching EU data protection law, it is crucial to keep in mind that only information that falls under the definition of personal data is effectively protected (White & Case, 2017). As stated previously, the definition can be found in Article 4 GDPR and encloses any information relating to an identified or identifiable natural person. Accordingly, data that is not considered personal data is not protected under the regulations discussed in this section. Moreover, before emphasis is put on the principles emerging from EU legislation on the protection of personal data, the term "processing" must be clarified. Processing essentially refers to all actions involving or affecting personal data to some extent. Article 4 GDPR provides a list of operations that fall under the scope of data processing and considers the collection, recording, organization, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure or destruction of data.

The legislation on the protection of personal data was updated only recently causing significant change in the field. Since the set of regulations entered into force on the 25 May 2018, the GDPR serves as key policy regarding the protection of personal data in the private and large parts of the public sector. It replaces Directive 95/46/EC and establishes a more ambitious standard of data protection. The

provisions of the GDPR are largely oriented towards strengthening citizens' fundamental rights in the digital age and simplifying rules for enterprises in the digital single market (Commission, 2018a). For example, the GDPR refines some of the key terms in the field of data security enhancing the scope of protection for European citizens. Moreover, the GDPR is composed to be a EU Regulation, making it one single law immediately enforceable in all Member States. This results in increased uniformity amongst the European Community and less administrative burdens as separate implementation in the Member States' national law is not required. In addition to the GDPR, the set of new regulations include Directive 2016/680 on Data Protection in the Police and Justice Sector, which is stressed in the subsequent section, as well as Directive (EU) 2016/681 on the Use of PNR data. The latter is subject of analysis in section 3.3 in chapter 3 of the study.

With the provisions of the GDPR, the EU has sharpened the data protection law considerably and correspondingly upheld respect for the fundamental right to privacy and data protection. Besides assigning rights to data subjects more extensively, for instance the right to erasure or the "right be forgotten" (Article 17 GDPR), it lists a revised version of five key principles for the governing of data proceedings in Article 5. These constitute an updated version of good practice guidelines for handling personal data (World Bank, 2018). According to the principles the data must be processed fairly, lawfully and transparent. Data may further be collected only for specific, explicit and legitimate purposes and processing is also required to occur in a manner compatible with the purposes. Moreover, data minimization refers to data being adequate, relevant and excessive in relation to the original purpose of collection. In terms of accuracy, data must relate to the purpose it was collected for. Hence, outdated data, that may have turned inaccurate over time, is required to be deleted. In addition, storage limitation ensures that data is not kept in a form which permits identification of data subjects for longer than necessary. Necessity is, in this context, defined according to the purpose underlying the collection of data in the first place. Lastly, data proceedings shall be characterized by integrity and confidentiality. This comprises, more precisely, the level of security from unauthorized and unlawful processing as well as from additional factors such as damage. Altogether, data may be proceeded only in accordance with a minimum standard of legitimacy. So, to ensure the lawfulness of the process, each principle is required to be fulfilled.

With the updated provisions of the GDPR, the EU grants for consistency with the obligations deriving from Human Rights frameworks and especially from Articles 7 and 8 CFREU, that have been discussed previously (*section 2.2*). The principles listed in Article 5 on data proceedings do therefore correspond with the on the principles identified for the protection of personal data, reflecting on the same fundamental values. For example, the lawfulness, fairness and transparency requirement of data proceedings is closely interlinked to the principle of transparency as applicant in data protection more generally. The GDPR hence translates key values and principles enshrined in Human Rights into European policy. The next section specifies these commitments on the basis of Directive 2016/680.

Because the potential impact data can have on the individual data subject is considerably high in the police and justice sector, data protection in the field is subject to specific regulations.

2.3.2. Directive 2016/680 on Data Protection in the Police and Justice Sector

Introducing the security dimension of the study, Directive 2016/680, also referred to as Law Enforcement Directive, is examined in the following. The Directive pursues a dual purpose as it aims on protecting citizen's fundamental right to privacy and data protection whenever personal data is proceeded as well as facilitating information exchange between competent security and law enforcement authorities within the EU. In this regard, it has legal validity on all natural persons regardless of their nationality. Subsequently this section outlines how the specific obligations incorporated in Directive serve its objective to ensure compliance with European fundamental rights in the police and justice sector. The provisions relating to data transfers to third countries are not subject of this section, since they will be exclusively discussed in section 2.4, which emphasizes international data flows in the security field.

Directive 2016/680 provides a set of common rules applicable for data transfers performed for a purpose linked to combating crime or terrorism. This may, more precisely, include the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties. The rules established under the Directive apply not only to domestic data proceedings but also to cross-border transfers within the EU. With its entry into force in May 2018, the Directive repealed Framework Decision 2008/977/JHA, which was the first standard setting EU legislation on data protection in the field of law enforcement cooperation. Guaranteeing a high level of protection for fundamental rights and freedoms, especially with regards to privacy and data protection, the scope of application of the Framework Decision has nonetheless been limited to cross-border proceedings and did not regulate data transfers on Member State's national level. Hence, with the new Directive a affects former gap in European legislation has been filled (Arthur Cox, 2016).

The objective of the legislators was to establish a legal instrument that would encounter technological developments and facilitate the conditions for law enforcement authorities to combat crime in the digital age more effectively and in compliance with present standards on data protection. With the CJEU's judgments in Digital Rights Ireland and in the Schrems case, EU policy makers have been assigned with concreate guidelines on how to ensure the respect to fundamental rights in the security and law enforcement environment (Coudert, 2016). The new legislation is further expected to make data sharing at the EU and international level more efficient, to increase trust amongst competent authorities and to guarantee legal certainty across borders (Commission, 2016a).

With Directive 2016/680, the EU has yet directed principles to apply for law enforcement for the first time. Article 4 of the Directive serves as appropriate legal base elaborating on these commitments. In accordance with Article 5 GDPR, the respect to lawfulness and fairness of data transfers is highlighted firstly. Due to the sensitivity and strategic value of information the field, transparency is however not

promoted. The additional provisions under Article 4 ensure legality, proportionality and necessity of data proceedings identical to the principles stated in the GDPR. All in all, European policy makers have with the Law Enforcement Directive successfully implemented a legal instrument which includes all EU internal police and judicial data processing activities under a common framework and at the same time maintains comprehensive respect to data protection rights within the EU.

2.3.3. The European Approach on Counter-terrorism

In this section the focus lies on the character of European counter-terrorism approaches. Since the 1970's the European Member States have sustained cooperation in the fight against terrorism. Over the years, the character of the cooperation has developed from comprising national objectives primarily towards a transnational alliance against the evolving terrorist threat. With the Maastricht Treaty, counter-terrorism has formally been included within the EU regulatory framework in 1992. Pertaining to the sphere of judicial and police cooperation in criminal matters which is established in Cooperation in JHA under the third pillar of the Treaty, counter-terrorism cooperation was subject to intergovernmental methods. Half a decade later, the entry into force of the Treaty of Amsterdam in 1997 and with it the introduction of the ASFJ have constituted the first key step in the direction of a more open stance in police and security cooperation. The 9/11 attacks then triggered a strategic rethink in the fight against the terrorist threat, which paved the way for the present character of cross-border cooperation. In the aftermath, the EU reinforced a new agenda on the threat by adapting a Framework Decision 2002/475/JHA on Combatting Terrorism as well as several action plans. It was however not until the incidents occurred on European territory in Madrid 2004 and London 2005, that counter-terrorism measures and instruments were put into decent formulation within the EU Counter-Terrorism Strategy, which has been subject of discussion in the introduction of the study. Prior to the mid-2000 events, the EU has primarily focused on internationally operating terror networks paying little attention to the possibility of domestic terrorism. Together with the concurrently adopted EU strategy for combating radicalisation and recruitment, the EU Counter-Terrorism Strategy postured a landmark in the European assessment of the threat within its border. Simultaneously, it illustrates the major concerns held by the EU and its Member States. Referring to the implementation of countering actions as "strategy" does further suggest greater consistency of the European approach in the fight against terrorism from 2005 onwards (Bakker, 2015).

Within the strategic framework, cooperative and coordinating measures are adopted on a large scale. These do not only pertain to internal cooperation, but also to collaboration with international partners. The European External Action Service lists joint efforts of the EU and the Member States for instance in one line with third country partnerships for the effective integration of internal and external counter-terrorism work (EEAS, 2016). Having developed into a separate policy domain within the EU, the counter-terrorism strategy has become an integral element of the AFSJ. Cooperation between national police and security authorities is however not only crucial in countering terrorism. The EU does, more generally, reinforce joint action as a key instrument for addressing criminal matters within the AFSJ.

The appropriate legal basis for cross-border law enforcement is found in Title V of the TFEU. Within the scope of the legacy, administrative and operational assistance between the Member State has constantly been strengthened, resulting in enhanced cooperation on the European level. The EU-wide harmonization of national policies is however excluded according to the provisions of Article 84 TFEU. This is because national security falls within the sole responsibility of the Member States (Article 4 TFEU). Therefore, consensus amongst Member States on a common agenda to fight terrorism does not equal a pan-European harmonization in the field (Edwards & Meyer, 2008). The engagement on the European level can rather be seen "as a complement to national efforts, where added value [is] possible and desirable." (Coolsaet, 2010).

In addition to intensified cooperation, the respect to human rights and the rule of law constitutes another main pillar of the European strategic guidelines in countering terrorism. The EU Counter-Terrorism Strategy and the updated Terrorism Action Plan thus promote a criminal justice approach on fighting terrorism whilst protecting human rights. EU Counter-Terrorism Coordinator Gijs de Vries notes, that the fight against terrorism in accordance with the rule of law is essential for democratic states as to avoid overreaction and compliance with terrorists' intentions to trigger extreme reaction on the European side (CVCE, 2007). The obligation to ensure fundamental rights is applicable within the Member States but also outside of the European borders, for example in countries receiving European support in addressing their domestic terrorism threat.

With regards to the digital age, special emphasis was assigned to privacy and data protection in formulating counter-terrorism guidelines recently. With the transformation of ICT, law enforcement and obligations on data protection become increasingly convoluted. According to the European Data Protection Supervisor, the EU's independent data protection authority, in a new political and legal environment "the scale of collection, storage and cross-border exchange of personal data between Member States in crime and terrorism matters is enormous." (EDPS, n.d.). Moreover, contemporary terrorism has become more digital too, relocating large spheres of their activity and communication to the internet. Therefore, the threat is nowadays even more diverse and multifaceted which makes the assessment increasingly complex. Encountering it effectively requires the EU to be exceedingly agile in their security and law enforcement. Included in this is also to realize the full strategic potential of data and information exchange, however within the boundaries of respective legal provisions. However, the closer the EU and the Member States are cooperating with each other and third countries, the greater the amount of personal data from EU citizens that is gathered, proceeded and retained. Considering the extensive volume of the datasets retained by global law enforcement bodies, one may refer to the accumulation as bulk data. Coincident with the enhanced collection of data, privacy concerns on maintaining full respect to data protection standards have increased. As having argued before with regards to law enforcement and countering terrorism, the EU is therefore in need to balance diverging interests of public security on the one hand and privacy and data protection as civil freedoms on the other. The European Data Protection Supervisor argues in this line by acknowledging the challenging

relationship between security and data protection in view of security authorities' broadened access to European databases (EDPS, n.d.). Taking everything into account, one can suggest the strategic guidelines in the ASFJ one of the biggest dilemmas of European counter-terrorism approaches (Bures, 2007).

2.4. Data Flows in International Security and Counter-terrorism Cooperation

This section builds up on the former contents by emphasizing data proceedings for security purposes as embedded in counter-terrorism cooperation between the EU and third countries. Thereby, it stresses the impact of EU internal data protection legislation on cross-border transfers. Increasing cooperation efforts with third countries in countering terrorism and criminal offenses have fostered international information exchange. The compliance to the principles emerging from Article 4 Directive 2016/680 on the processing of personal data is required in any case. Data transfers to non-European countries must correspond with them to allow the proceeding taking place.

For maintaining full respect to privacy and data protection, the EU has additionally established various safeguards to ensure that data and its European standard of protection travel together. Generally, data transfers outside of the European Economic Area (EEA) are prohibited (Arthur Cox, 2017). Under certain conditions however, transfers may take place. Chapter V of the Law Enforcement Directive contains a set of provisions determining the legal conditions for transfers of personal data to third countries and international organizations outside of the EEA.

Accordingly, Data may be transferred on the basis of an adequacy decision. The concept has been defined by the CJEU in the Schrems case, however in the context data transfers for economic purposes (Schrems v Data Protection Commissioner, 2015). Because it is a key element in determining the external dimension of the study, the adequacy decision is analyzed more profoundly in Chapter 5.2.1 of the study. In the security field, Article 36 of Directive 2016/680 ensures the information receiving country to warrant an adequate protection standard. The Commission must have confirmed that fundamental rights and freedoms concerning data are guaranteed by the receiver's legislative framework prior to the data transfer taking place. From a linguistic viewpoint, the term adequacy does in this context refer to countries having a domestic approach to data protection similar to the European one. The evaluation of the level of data protection is based on a set of elements embedded in Article 36 (2), including for example the respect to fundamental rights and freedoms. It does not only touch upon the existence of appropriate legislation but also considers to what extent these are implemented in practice. This reflection on the factual level of data protection in a third country is an additional safeguard provided for in the Directive. In the absence of an adequacy decision, Articles 37 and 38 allow data to be transferred outside of the EU pursuant to specific safeguards or a derogation.

Due to the traditionally close partnership between the EU and the US, this section puts special emphasizes on the law enforcement cooperation while stressing the character of the national data

protection regimes. Information exchange is a crucial component underpinning the transatlantic relationship. It necessarily requires a high level of protection in accordance with privacy legislation (Commission, 2015). In 2013, the Snowden revelations on unlawful data collection by US intelligence agencies have raised serious concerns amongst the EU and its Member States. These were primarily expressed in relation to large-scale data proceedings of European citizen's data by private actors, but also by public bodies including security authorities (Commission, 2016b). In response to the 2013 reports, data protection safeguards for transnational law enforcement cooperation has been strengthened by negotiation the EU-US Data Protection Umbrella agreement. The agreement shall rebuild trust in the transatlantic partnership and ensure better protection of transferred data, although not allowing the transfer as such. The European Council hence signifies the agreement as "as a complement to existing and future agreements." (European Council, 2018). Generally, the European approach on data protection differs from the assessment prevalent in the US. Since the differences have been subject to extensive analysis by many scholars, a detailed examination is not reasonable at this point considering the limited scope of the study. As argued previously, the EU demonstrates full responsibility to respecting privacy and data protection, whereas the US are proclaimed to hold less extensive standards in the field (Dimitrova & Brkan, 2018). Ultimately, to understand the transatlantic partnership, acknowledging the fundamental differences in both legal and regulatory frameworks is required.

2.5. Conclusion on Data Protection and Data Flows in the Fight against Transnational Crime and Terrorism

In the previous sections, the European stance on privacy and data protection as fundamental rights has been outlined. In addition, the strategic value and handling of data in EU counter-terrorism approaches has been elaborated by emphasizing data transfers in the law enforcement sector. This section clarifies the relationship between the provisions on protecting personal and counter-terrorism cooperation with third countries and answers the first subquestion of the study: Which protection standards apply on the processing of personal data in the European security environment and how do they affect counter-terrorism cooperation with third countries?

Data protection standards in the EU as emerging from human rights frameworks do in general ensure a high level of protection, which is secured through various safeguards to be found in most policies concerning data proceedings. Although the rights to privacy and data protection may not be absolute, the EU assigns them great importance in view of other, possibly interfering rights. The European data protection legislation further provides guiding principles applicant on data proceedings within the EU but also outside of its Member States borders. Standards established in this context are designed according to the rule of law, proportionality, necessity and appropriateness. As the European approach on countering criminal offenses and terrorism strives for compliance with the protection of citizen's persona data, the principles have been implemented in the field of law enforcement as well, although under the presence of some adjustments for example with respect to transparency. Regarding the

practical dimension of data processing, the relationship between security aims on the one hand and privacy obligations on the other, increases the potential for interest clashes. With the entry into force of the GDPR and the law enforcement Directive, the EU has managed to implement coherent regulations, that determine the scope of action for security authorities on legal grounds. This marks an important contribution to the fight against terrorism in accordance with the EU counter-terrorism strategy.

Emerging from this chapter, borderless data flows and internationalization of crime and terrorism require cooperation across borders between the EU and third countries. This cooperation must, in accordance with the Treaties and the CFREU, ensure the protection of civil rights and freedoms, including the rights to privacy and data protection. In this vein, the adequacy decision has become a key instrument to determine the respect of data receiving countries or organizations to these rights. Together with the provisions stated in Article V of the Law Enforcement Directive, it imposes conditions on the lawfulness of international data flows. Nevertheless, in the security environment there exist numerous regulations proposing regulations on specific circumstances. The use of PNR data in law enforcement is one of the domains in which rules for the proceeding have been stated explicitly. Therefore, PNR data is studied in detail in the next chapter.

3. THE EUROPEAN LEGAL FRAMEWORK ON PNR DATA

3.1. Introduction to the European Legal Framework on PNR Data

Having outlined the foundations of security and privacy, PNR data is examined next. Hereby, the focus lies on the European internal perspective to introduce the case study on PNR data. The chapter aims on concluding an answer to the subquestion: What is the existing regulatory framework on PNR data within the EU and does it provide sufficient protection safeguards?

In contrast to Advanced Passenger Information (API), concerning data from passport's machine-readable parts, such as the document number or nationality, PNR is a unique dataset that contains information on key components of flight reservations made by natural persons. The information consists of 19 categories, covering for example contact details including addresses, payment information and number of persons travelling. It thus provides a border information range than conventional API, proving useful in discerning passenger's intentions. On that basis it enables security enforcement authorities risk assessment of unrecognized terrorists and criminals but also the identification of known individuals. In this aspect, PNR data may be used either in the aftermath of a committed crime or proactively to determine high-risk passengers (European Parliament, 2015b). This makes PNR data a highly effective tool in the field of law enforcement. Most relevantly, the collection and use of the data marks an essential measure in fighting cross-border crime, including children trafficking but also acts of terrorism. Additionally, foreign fighters returning to Europe from IS occupied territory may be detected more sufficiently using PNR data. According to this perspective, the strategic value of PNR seems to justify the transfer and proceeding of passenger's personal information in general. However, the collection of massive amounts of personal data remains the reverse side of the method.

For this chapter to provide a comprehensive picture on the European PNR system, the legislation governing PNR data proceedings is encompassed firstly (*section 3.2*). Since the entry into force of the data protection reform package in May, Directive 2016/681 serves as legislative basis for the PNR data system governing the transfer of PNR data on all extra-EU flights entering or departing from EU territory as well as the processing of the information by competent authorities. The section provides background knowledge by identifying key factors that have resulted in the adoption of the Directive in its present form. Because PNR data constitutes personal data in the meaning of the Article 4 GDPR, there are specific protection safeguards embedded in PNR data legislation, that are also presented in the section. Subsequently, emphasis is shifted to the reverse side of PNR data (*section 3.3*). The practice has caused controversial discussions on data protection safeguards and thus on fundamental rights compliance of Directive 2016/681. Given this, the section scrutinizes the rights at stake on the grounds of proportionality and necessity. On that basis, a conclusion on European PNR Legislation is formulated afterwards (*section 3.4*).

3.2. Legislation on PNR Data

Member States have in fact used PNR data for law enforcement purposes, either on the basis of national legislation or general legal powers, before Directive 2016/681 has established common rules (Council, 2016). With the new regulatory framework, greater harmonization in the area is to be facilitated for enabling the systematic collection and use of PNR data for the prevention, detection, investigation and prosecution of terrorist offenses and serious organized crime across Europe. The PNR Directive specifically regulates the transfer of passenger's PNR data of EU international flights from air carriers to the Member States as well as the processing of such data between European Member States and third countries. The transfer of data from a Member State to a third country is governed by Article 11 that introduces a set of provisions allowing for the transfer on a case-to-case basis. Accordingly, the transfer may take place only provided that the Member State has ascertained the data receiving country to proceed data in accordance with the Directive's aim and to guarantee sufficient protection safeguards in its domestic law. In addition to Article 11, Article 21 of the PNR Directive ensures that other data sharing instruments remain in force given their compliance with the Directive. This affects bilateral PNR data sharing agreements that have been negotiated on the EU level but also bi- and multilateral agreements on data sharing concluded between EU Member States and third countries on the basis of Article 4 TFEU. Until the recent introduction of the data protection reform package, the field of data processing in the police and criminal justice context was left outside of EU law, which is why some EU Member States hold individual agreements with third countries. These existing agreements shall persist without prejudice to any obligations and commitments of the Member States or the EU. In fact, this provision compromises interests on the requirements on law enforcement and criminal justice work as well as the requirement for enhanced data protection safeguards on the EU level (Di Francesco Maesa, 2016).

In Chapter I of the Directive 2016/681 general provisions on the scope of the legislation, the optional application to intra-EU flights and further definitions are provided. Chapter II encompasses the Member States responsibilities under the PNR Directive. These include various data protection safeguards such as details on data processing and retention periods. For dealing with data management, Member States are for instance required to establish a national Passenger Information Unit (PIU) which receives data from the air carriers and holds responsibility for data storage, analyzation according to a set of predefined criteria and referral to designated competent authorities (Article 4). After 6 months of initial storage at the PIU, the data is systematically masked out and stored anonymized for another period of four and a half years (Article 12). Hereafter, the Directive contains implementing measures with regards to common protocols and data formats in Chapter III and presents final provisions in Chapter IV. Lastly, items of personal data covered under PNR are listed in Annex I and offenses considered serious crime are specified in Annex II.

After previous drafts of the PNR Directive were rejected by the European Parliament due to serious concerns on individual data privacy, the legislative process has been on hold until the Paris terror attacks

in 2015. The events drew back attention to the demand for effective measures in fighting the terrorist threat, causing EU officials to relaunch action to establish an European-wide PNR system (Eclan, 2016). Given the event-oriented revival, Bigo et al. (2015) argue that with the PNR Directive "rapid and emergence-led policy responses have […] taken precedence over quality and democratically (rule of law) accountable decision-making.". Although this might be true to some extent, the quality of data protection safeguards in the PNR Directive has benefited from developments on data privacy in the domain of JHA. Primarily caused by the Snowden revelations, the demand for better data protection obligations was acknowledged by the CJEU judgments in Schrems and Digital Rights Ireland. Especially the decision in Digital Rights Ireland has led to considerable implications in designing the final form of Directive 2016/681 in favor of data security. In the envisaged case, the CJEU declared the collection of bulk data by Member States' intelligence and security authorities invalid with EU data protection principles deriving from EU primary law. In that sense, the CJEU formulated a set of requirements valid for law enforcement instruments interfering with privacy and data protection. It was stated that data retention can put into practice only under full respect to proportionality and necessity and according to an objective of general interest. In case-law, for example in Tsakouridis (Land of Baden-Württemberg v. Panagiotis Tsakouridis), fighting terrorism and serious criminal offenses for maintaining public security were recognized as objectives incorporating general interests (Di Francesco Maesa, 2016). Moreover, compliance with the proportionality and necessity obligation is ensured through the adoption of additional safeguards in the PNR Directive that have not been embodied in previous drafts. These include, for example, the appointment of a national data protection officer, who is responsible for monitoring PNR data processing and implementing relevant data protection safeguards (Article 5). Also, for limiting the overall scope of the PNR Directive, the list of criminal offenses to fall under the Directive's scope was narrowed and the overall data retention period was shortened.

All in all, the PNR Directive reflects a set of requirements essential in guaranteeing for the lawful proceeding of PNR data. In case-law, the CJEU has imposed substantial instructions on EU policy makers that have been adopted in designing the PNR Directive (Loewe, 2016). Key for the legislation is that it incorporates specific safeguards to ensure full respect to EU data protection law as well as effective assistance in preventing acts of terrorism and criminal offenses. As Blasi-Casagran (2017) points out, the Directive is in fact the only data-sharing instrument in the EU that pays full respect to all basic rights stated in Directive 95/46 EU, including for instance the right to free data access and judicial redress (Article 13). However, since the PNR Directive has entered into force only recently, its effect in practice remains yet to be seen. As imposed by Article 19, the application of the Directive's provisions is to be monitored by the Commission. Thereby, particular attention is advised to the compliance with the applicable standards of protection of personal data, the proportionality and necessity of collecting and processing PNR data, the length of the data retention period and the effectiveness of exchange of information between EU Member States (Article 19.2). On the 25 May 2020, exactly two years after the PNR Directive entered into force, the first review report will be published.

3.3. Controversy over the Use of PNR Data in Law Enforcement

Directive 2016/681, as a law enforcement tool, aims on ensuring public security through the use of personal PNR data. As outlined above, data protection safeguards inhabitant in the PNR Directive have been facilitated increasingly during the EU legislative process. Nevertheless, not all concerns on the Directive, especially with regards to data protection, have been met entirely. The PNR Directive lacks for instance any mention of fundamental rights, which poses a critical point regarding its impact on these freedoms (Di Francesco Maesa, 2016). In the following section the rights at stake are outlined. Firstly, the EU PNR system is suspected to undermine the fundamental rights to respect for private life and to the protection of personal data, emerging from Articles 7 and 8 CFREU. Since the PNR Directive affects all passenger of extra-EU flights regardless of any evidence suggesting them to be involved into acts of terrorism or serious crime, it leads to large scale surveillance and systematic monitoring of personal data. In that sense, voices against the legislation proclaim an expanding surveillance society (Loewe, 2016; Vavoula, 2016). Moreover, systematic collecting and analysis of all passenger's personal data is problematic in light of the right to non-discrimination, stated in Article 21 CFREU. Profiling measures incorporated in the PNR system might "lead to the unfair targeting of European citizens with a second ('foreign') nationality or foreign background." (Bigo et al., 2015). Furthermore, Directive 2016/681 does not contain any details on the criteria according to which profiling operations are performed (Di Francesco Maesa, 2016). This is especially questionable in terms of transparency. Lastly, Member States may additionally apply the PNR Directive to intra-EU flights provided that they notify the Commission about their action (Article 2). The extension may result in restricting the right to free movement on grounds of public security (Di Francesco Maesa, 2016). Since a number of rights might be conflicting with the provisions of the PNR Directive, the voiced reservations on the European PNR approach seem reasonable.

To approach the delicate relationship between fundamental rights and the EU PNR system in more detail, it is crucial to reconsider the legal criteria of proportionality and necessity. In Article 52 CFREU the principle of proportionality is recognized for any limitation to fundamental rights and values stated in the Charter. Since PNR data proceedings are indeed tangent to CFREU rights, it is necessary to ensure appropriate proportionate safeguards. The main instrument in doing so is the purpose limitation. Accordingly, data proceedings are supposed to serve a specified, explicit and legitimate purpose. Any further transfer not compatible with the formulated purpose is strictly prohibited (Article 29 Working Party, 2013). When applied to the PNR Directive, the purpose lies in the protection of public security against terrorist offenses and serious crime. The necessity principle takes up on this, as it is determined by the effectiveness of the measures selected to fulfill the underlying purpose (European Parliament, 2015b). Thus, necessity is dependent on how well suited the PNR Directive is for fighting acts of terrorism and serious crime. As stated previously, the practical effect of the European PNR system is not to be determined yet. Moreover, relevant statistics on the relationship between PNR systems and public security are not available. Only national examples, such as the UK e-Border system, provide

some evidence for the successful use of PNR data in the fight against terrorism and crime (Brouwer, 2011). However, under consideration of the interfaces between terrorism and air travel outlined by Loewe (2016), the transfer of PNR data for safeguarding public security is lawful according to the proportionality test. Controversies on the PNR system arise especially from legal subtleties of Directive 2016/681, including the retention period of five years, the nature of data anonymization and retrieval procedures. In addition, the possibility of gradual use expansion of the PNR system is subject of heavy criticism. Once individual's PNR data is stored in a European-wide system, the probability that the initial purpose of data proceeding is legally expanded, increases (Blasi-Casagran, 2017).

3.4. Conclusion on European PNR Legislation

This chapter has analyzed the European legal framework on PNR data by assigning special emphasis on Directive 2016/681. The legislation governs the collection of PNR data by air carriers for all extra-EU flights entering or departing from the EU, as well as the transfer of such data to EU Member States and sharing mechanisms across borders. The chapter has deepened the understanding on how the Directive was constituted in its prevalent form on the one hand and on the points of tension between fundamental rights protection and public security. After all, the lawfulness of Directive 2016/681 remains subject of legal interpretation according to the principles of proportionality and necessity. Since the Directive has, however, entered into force only recently an analysis on its practical effect may not be performed yet. Its factual impact on PNR data proceedings does thus remain to be seen within the next years. Despite the points of criticism stressed in the previous section, many scholars have in their analysis found the PNR Directive to be an appropriate law enforcement instrument due to the inclusion of substantive and precise safeguards against the abuse of individual's personal data (Knight, 2016; Di Francesco Maesa, 2016). By imposing strict conditions on proportionality and necessity of PNR data proceedings, that have been studied in this chapter, EU legislators have provided sufficient procedural safeguards for the protection of passenger's data in the legislation.

With regards to the level of implementation of Directive 2016/681 the Member States reveal considerable differences in transferring the new regulations into domestic law. Not all Member States have yet finished to fully meet the PNR Directive's obligations, despite substantial efforts from the EU in supporting the implementation through financial assistance. In 2017 alone, the Member States have received 70 Million Euros funding for the development of national PNR schemes and related PNR activities (Commission, 2018b). In a statement issued by the Commission, the significance of functioning PNR systems across all EU Member States is highlighted, since "[i]n the fight against terrorism and organised crime, Europe cannot afford weak links" (Commission, 2018b). With this, the Commission underlines its willingness to exercise all competences under the TEU and TFEU to ensure that reasonable progress is made in due course. In any case, with the adoption of the PNR Directive, the EU aimed on closing an important security gap that allowed terrorist and other criminals to enter and travel freely within EU territory. Although the Directive might not stop the travels entirely, it can

function as a deterrent measure. In this chapter, evidence was presented that in implementing this objective, the Directive incorporates not only sufficient procedural safeguards. In addition, data is proceeded with specificity to ensure compliance with the European rule of law. Therefore, PNR data practice within the EU is generally in line with the fundamental rights to privacy and data protection. Nevertheless, it needs to be noted that this tendency does not equal Directive 2016/681 to ultimately ensure full protection to the PNR data of European citizens. Perspectively, the legislation will need adjustments, for example in aftermath of the first policy review.

4. THE JURISDICTION ON EUROPEAN PNR DATA TRANSFER AGREEMENTS WITH THIRD COUNTRIES

4.1. Introduction to the Jurisdiction on EU PNR Data Transfer Agreements with Third Countries

The external dimension of PNR data is approached by envisaging the agreements in force between the EU and third countries. PNR data may be transferred to a third country only for law enforcement purposes and on the basis of a bilateral agreement that guarantees a high level of security for personal information through sufficient data protection safeguards (Commission, n.d.). Due to the share of competences in the ASFJ deriving from Article 4 TFEU, not only the EU may conclude such third country agreements but also the Member States. Although, none of the Member States has exercised the right to negotiate a PNR data transfer agreement with an EU-external partner, national engagement in international security cooperation is not entirely omitted. Most commonly, the cooperation is fostered within a bi- or multinational memorandum of understanding (MOU). In contrast to an agreement, a MOU is not legally binding. Nevertheless, it demonstrates considerable cohesion and mutual respect between the parties involved. Currently, countries including the United Kingdom, Germany and Greece have signed bilateral MOUs on the exchange of travelers' data with US security authorities. As not all MOUs necessarily involve the transfer of PNR data and because of the study's European focus, this chapter solely emphasizes the international agreements on PNR data proceedings that have been negotiated by the EU. Unlike the previous chapter that has studied PNR from an EU internal perspective, the following sections expand the scope of the study to the EU external dimension. To this date, the EU has signed PNR data transfer agreements with the US, Canada and Australia. Although, negotiations on another PNR agreement with Mexico have started in 2015, a final conclusion has not yet been reached. Moreover, the Commission has stressed its intentions to conclude additional agreements with key countries (Commission, 2017b). Perspective candidates for further agreements include, for example, Japan and Argentina (Vedaschi & Graziani, 2018). Considering that in Chapter 2 it was concluded that joint intelligence actions and strategic partnerships are essential for fighting the rising terrorism threat effectively, efforts to establish other international PNR agreements seem sound. However, to that day, the introduction of PNR agreements has remained a sensible matter, especially due to concerns in relation to the level of respect to fundamental rights in data receiving third countries, particularly to the right to privacy and data protection. Alike Directive 2016/681, international PNR transfer agreements are subject to strong criticism from non-governmental organizations (NGOs) engaged in the field, but also from Members of the European Parliament (MEPs). Both parties claim on privacy and anti-discrimination violations, a lack of transparency and the departure from the general presumption of innocence. To date, the EU has not reached consensus on how to meet the wide-ranging concerns.

For approaching bilateral agreements governing the external transfer of PNR data from the EU to third countries' security authorities, factors that have historically shaped the conclusion and development of such agreements are outlined first (*section 4.2*). The EU-US agreement demands some extra attention

resulting from its guidance role in the history of PNR agreements. As previously stated, in the aftermath of 9/11, US security authorities started to use PNR data for law enforcement purposes. The US Aviation and Transportation Security Act of 2001 conditioned the access to travelers PNR data for all foreign airlines flying into the US. This created a situation in which EU air carriers faced the dilemma of either violating US law or, alternatively, EU data protection requirements deriving from European airline obligations and Article 25 of Directive 95/46 (Blasi-Casagran, 2017). With the introduction of the first PNR agreement, negotiated between the EU and the US in 2004, the Commission, thus, intended to implement a legal basis for the processing of PNR data in European law (Papakonstantinou & de Hert, 2009). The newly established Directive 2016/681, that has been subject of discussion in the previous chapter, does constitute the latest development on the path of PNR history. Although the Directive pertains EU internal legislation, effects on third country agreements in the external dimension may not be precluded. Therefore, the relationship between the Directive and the bilateral PNR agreements in force is also analyzed in section 4.2.

When studying the existing agreements, strong interrelations in terms of structure and provisions become evident. Consequently, a profound analysis of the three bilateral PNR agreements in force is necessary (*section 4.3*). This study aims on elaborating key protection principles underlying the transfer of PNR data. Thereby, it simultaneously covers all agreements by assigning special emphasis on the exploitation of legal gaps in the agreement's data protection safeguards. For the analysis, special categories covering the main elements of the PNR agreements, such as use and purpose of the data, domestic share and data retention period, are grouped. Finally, an answer to the third subquestion is given: Which principles for international data transfers emerge from PNR agreements between the EU and third countries (*section 4.4*)?

4.2. Development of External PNR Agreements with Third Countries

The history of international PNR agreements reaches back to the 2001 terrorist attacks in the US. In the aftermath of the event, the Western world agreed on setting up a new security strategy to ensure better protection to the life and safety of the public. The primary objective of the strategic realignment was the prevention of a further incident similar to 9/11. The US, being most-affected by the attacks, acted as the main driver of the renewed security orientation calling for stricter controls in civil aviation travel. In that role, American security authorities started to make use of PNR data in the law enforcement context. Concurrently, third countries were pressured to follow the same line by adopting new US law, namely the US Aviation and Transportation Security Act of 2001. It obliged foreign air carriers to warrant US authorities access to PNR data from passengers entering or leaving the US. The monetary sanctions implemented under the law caused indirect, albeit considerable, pressure to the EU Commission, that was further increased by legal uncertainty among European aviation companies. This duress is considered the main factor in leading to the conclusion of the first-ever EU US PNR agreement (Taylor, 2013). Besides, it was intended to restore legal certainty in the aviation industry. Negotiations on further

bilateral PNR agreements with Canada and Australia followed, resulting in completions in 2006 and 2008.

Today's PNR agreements are, however, rather second and third generation agreements. Although the Commission argued in favor of fundamental rights compliance and a high level of personal data protection provided for in the agreements, concerns regarding the lack of privacy and data protection safeguards remained across the civil society and within the Parliament. Eventually, these concerns reached a dimension on which the Parliament sought the opinion of the CJEU that annulled the EU-US agreement in 2006, declaring its conclusion was ultra vires and, thus, lacking an appropriate legal basis (Joint Cases C-317/04 and C-318/04). However, reference to whether the agreement violates fundamental rights was not made in the judgment. In compensation for the first-generation EU-US agreement, a provisional seven-year agreement was concluded in 2007 that did not embrace modifications on the protection of personal data. Therefore, the persistent concerns resulted in the Parliament pressing the Commission to issue a reconsidered strategy on external PNR data proceedings to the US, Canada and Australia in 2010 (Commission, 2010). The Commission's Communication on the global approach to transfers of Passenger Name Record data to third countries recognized the challenges that emerged from major data protection concerns on PNR data processing to third countries in the security context and desired to define a consistent framework of basic principles valid for future external PNR agreements. On the one hand, the document aimed on the reduction of legal uncertainties and administrative burdens for European air carriers and Member States resulting from different requirements stated in the bilateral PNR agreements at that time. On the other hand, it emphasized improved redress and more effective legal safeguards to meet the reservations on respect to privacy and data protection. For these purposes the Commission set out a list of general criteria applicable for future bilateral PNR agreements, including, *inter alia*, a change in the transmission method (from pull to push), specified obligations with regards to transparency and adjustments to the data retention period. Moreover, the document fostered the compliance of external PNR data proceedings with the principles of proportionality and necessity by stating, under the first point, that the use of data should be limited to the purpose of the transfer and secondly, that only the minimum of necessary data should be exchanged. In that line the onwards transfer of European citizen's PNR data from the data receiving country to other third countries was restricted under the renewed approach. The Commission also announced to review the external PNR agreements on a regular base and to put mechanism for monitoring their implementation, application and interpretation into place. From today's perspective, EU and foreign authorities progress well in this regard. For instance, joint evaluations on compliance with the standards in the agreements are carried out repeatedly as well as binational delegations conduct regular joint review visits (Commission, 2017c). Reactions on the Commission's Communication were mainly positive. Even stakeholders known for being in favor of strict data protection mechanisms, such as the Article 29 Working Party, generally welcomed the paper as a step in the right direction (Article 29 Working Party, 2010).

Based on the general criteria formulated under the 2010 strategy, the Commission issued three proposals aiming on implementing the legal renewals into the external PNR data transfer agreements. The improved EU-US agreement was concluded in 2012, followed by a revised EU-Australia agreement later that year, both under the approval of the Parliament. Despite formal distinctions in the design of the EU-US and EU-Australia PNR agreements, the Parliament recognized the overall compliance of the provisions with the set of principles formulated under the Commission's Communication of 2010. However, with regard to the agreement on the use of PNR between the EU and Canada, the Parliament did not permit its required consent on the conclusion of the contract in 2014. Contrary, it voted on seeking an Opinion of the CJEU under Article 218(11) TFEU as to clarify the compatibility of the draft agreement with the EU legal framework and the CFREU. According to Article 218(11) TFEU, an agreement may not come into effect in the event of not fully satisfying fundamental human rights standards. The next step in the history of bilateral PNR agreements was constituted by Opinion 1/15 of the CJEU, that has been referred to throughout the study several times. In its judgment, the CJEU declared the envisaged EU-Canada PNR agreement invalid in 2017. Although a profound analysis of the agreement's legal rejection under Opinion 1/15 is provided in section 5.2, at this point it is to note, that the CJEU refused the adaption of the envisaged agreement, stating that it had the wrong legal basis and that several of its provisions were incompatible with European fundamental rights.

Regarding the effects of Directive 2016/681 on the external PNR agreements, it seems like European policy-makers have endeavored to synchronize the new legislation's regulations with the general tenor of the third country agreements instead of reviewing the current approach towards PNR data proceedings in light of Opinion 1/15. The clauses of Article 11 of Directive 2016/681 do not obtain any aggravations on cross-border data transfers. Rather than introducing stricter provisions or enhanced protection safeguards, the Article builds on existing regulations deriving from Framework Decision 2008/977/JHA and confirms the legal integrity of the PNR agreements in force. Hence, one may not confirm any effect of Article 11 on bilateral PNR data transfer in practice. It seems like in designing the PNR Directive, EU legislators had no intentions to factually affect the external dimension of PNR data transfers. By avoiding confrontation with its strategic partners, the EU leaves the conclusion of effective changes in bilateral PNR data practice between the parties involved dependent on negotiations. Thereby, the EU, under international peer pressure, prioritizes the legal force of PNR data as a security and law enforcement tool over the respect to fundamental rights protection.

4.3. Analysis of External PNR Agreements with Third Countries

As above-mentioned, the Commission aims on highlighting the full compliance of the external PNR agreements with European fundamental rights and freedoms (Commission, n.d.; Commission, 2015; Commission 2018b). However, is the factual effect of these safeguards corresponding with the Commission's affirmations? For the analysis to capture the entire scope of the bilateral PNR agreements in force, the upcoming section requires to go beyond formalities by providing an in-depth study of

elements in the agreements that remain vague and without further specification. The main purpose of the analysis lies in the identification of legal gaps embedded in such provisions. These gaps may leave room for third countries to implement practice that interferes with European privacy standards and, in that line, erodes public trust in the European constitutional framework. As outlined previously to approach the external PNR agreements in a systematic manner, the most important factors have been grouped in categories, covering the most essential elements of the agreements. Importantly, this study scrutinizes the 2014 draft agreement between Canada and the EU on the transfer and processing of Passenger Name Record rather than the 2006 agreement to preserve the most topical picture in the analysis and to prime the study of Opinion 1/15.

Regarding the purpose and use of PNR data usage, the key notion of all agreements lies in the fight against terrorist offences and serious crime as being related to national security objectives. The EU-US agreement, in contrast to the EU-Canada and EU-Australia agreement, introduces a broader scope of what is considered terrorism under Article 4(1). A catalogue of examples is given, that includes, *inter alia*, hostage-taking or kidnapping but also all activities falling under the definition of terrorism given in international conventions and protocols. The choice of wording "*including conduct that*" leads to the impression that the definitions stated in Article 4(1)(a) are only examples of what is covered under acts of terrorism. Although all agreements leave room for legal interpretation by not providing an exact list of terrorist offences, the EU-US agreement sets the area of application the broadest through the wording. The definition of transnational crime is also left rather vague. Article 4(b) defines serious crime as any act punishable by a minimum sentence of imprisonment of three years but lacks reference to the exact legal system which defines the sentence. This leads to legal uncertainly regarding the application of the provision. The PNR agreement with Australia demonstrates a more comprehensive way in this regard by clearly referring to Australian law as correct legal basis in Article 3(3). In addition, Article 4(1)(b)(v) of the EU-US and in Article 3(3)(e) of the EU-Canada agreement define a crime of transnational nature as committed in one country, with the offender of the respective crime holding intentions to travel to another country. This, in literal interpretation, does also include journeys with no relation to the crime committed, such as holiday trips. Article 4(2) of the EU-US agreement further permits the use of PNR data on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court. This provision entirely lacks reference to the purpose of fighting terrorism or serious crime and, thus, opens the way to use PNR data in every law enforcement case provided that a court has decided to do so. Similarly, albeit less intrusive, Article 3(4) of both, the EU-Canada and the EU-Australia agreement, allow PNR data usage in exceptional cases, that are rather acquainted to terrorism and serious crime. In conclusion, the purpose and use of PNR data as stated in the external agreements is very wide-ranging, with parts of the EU-US agreement seriously undermining the principles of proportionality and necessity in the context of PNR data usage.

The retention of PNR data has always been a sensible matter in respect of privacy and data protection. In the external PNR agreements, the negotiation parties have agreed on a five to five-and-a-half-year

retention period for depersonalized PNR datasets. In presence of ongoing investigations this period may be extended unlimitedly according to Article 16(3) of the EU-Australia agreement. Article 16(5) of the EU-Canada agreement does further allow an extension if required for, *inter alia*, any specific action. The term is not specified, which leaves the paragraph's scope extremely broad. With regards to the EU-US agreement, Article 8 regulates that PNR data, after being retained in an active database, is forwarded to a dormant database for up to 10 years where it may be re-personalized from given law enforcement operations on identifiable cases, threats or risks (Article 8(3)). All in all, the data retention period anchored in the agreements leaves much room for circumstances under which data is not deleted after the initial period.

The domestic sharing of PNR data relates to the onwards transfer from the data receiving government authority to additional national authorities. In Australia, the onwards transfer may occur on case-by-case basis until the data is depersonalized (Article 18(1)(c)). This implies, however, that thereafter domestic sharing is permitted in an enlarged number of cases, as long as these relate to the purposes stated in Article 3. Moreover, the list of domestic authorities that may receive PNR data can be extended unreservedly according to Article 18(2), for example if functions of preexisting departments become directly related to the fight against terrorism and criminal offenses (Article 18(2)(c)). The agreement remains silent on reasons and backgrounds for such a rise of new functions. In any case, Article 18(2) paves the way for a subsequent extension of authorities, competent to receive and proceed PNR data of European citizens. The draft agreement between the EU and Canada yet entails no specifications on neither the competent authority for receiving PNR data as referred to in Article 2(d) nor on authorities to which PNR data may be transferred to according to Article 18. Although Article 30 ensures that the EU receives notification on which authorities are allocated to PNR-related tasks, it does not provide any further say to the EU on the choice of the authorities. If the agreement would have entered into force in this draft version, Canada could have extended the number of national authorities entailed to receive EU PNR data unlimitedly and without any control from the European side. In the EU-US agreement domestic sharing of PNR data is generally permitted in Article 16. Thereby, the agreement lacks any specification of the authorities entitled to receive PNR data. Consequently, the Department of Homeland Security may pass on PNR data to any American government authority given consistency with a purpose included in Article 4. Following the conclusion above, the purposes covered under Article 4 are extremely broad, thus, the safeguard remains without great effect. Considering the overall provisions on domestic PNR data sharing embedded in the agreements, it can be concluded, that the incorporated restrictions and safeguards are subject to several far-reaching exceptions, that may lead to considerable data protection constraints.

In connection, onwards transfer to other third countries, for instance, from the US to Mexico, is permitted in all agreements under specific circumstances. According to Article 19 (1)(e) of the EU-Canada agreement and Article 19 (1)(a) of the EU-Australia agreement, the respective competent authority is required to obtain satisfaction with the data protection standards prevalent in the third

country in advance to the onwards transfer. The criteria conditioning satisfaction in this context are, however, not specified any further. Only, the EU-US agreement includes an additional provision on ascertaining that the recipient's intended use is consistent with the agreement (Article 17(1)). Concrete measures on how to control the recipient's usage is not outlined. Therefore, the safeguard remains rather blank. Furthermore, in what is described as an "*emergency situation*", the US permits onwards transfer of PNR data to additional third countries conceding that the recipient may not provide a sufficient standard of protection (Article 17(2)). Clearly, the practice accepts the violation of European fundamental rights in favor of national security. This is particularly problematic as the agreement lacks a clear definition of emergencies. Consequently, the onwards transfer to other third countries is highly questionable. As it is not subject to prior judicial authorization, the level of privacy as well as the compliance with EU standards in an additional third country cannot be guaranteed with certainty. Therefore, the risk of data protection violations increases significantly.

Although all agreements recognize respect to privacy and data protection, only the EU-Australia agreement declares PNR data subject to the Australian Privacy Act's provisions (Article 7.1). The other agreements remain silent on specific legislations that condition incorporated safeguards. Such missing details increase the level of incoherence within the envisaged agreements. Additionally, in light of data security and integrity, the scope of protection provided differs considerably among the agreements. In contrast to the agreement with Canada, the EU-Australia agreement acknowledges more activities under unlawful forms of processing, for instance, alteration or unauthorized disclosure (Article 9(1)). Special interest lies in the sanctions for any kind of unlawful processing that are provided in the agreements. While the agreement with Australia in Article 9(2) affirms sanctions of effective and dissuasive nature, the agreement with Canada in Article 9(5) softens this element by announcing "*corrective measures, that might include sanctions"*. The wording implies that breaches of data security may remain without any consequence to the responsible executive. Nonetheless, the EU-US agreement provides for the lowest level of security in this regard. Even though measures may be taken in the aftermath of a privacy incident, these remain superficial and little comprehensive (Article 5(3); Article 5(5)). The term sanction is not to be found in the entire EU-US agreement. Besides, any improvements on data protection may be ruled out on basis of Article 21, according to which the agreement shall not confer any new right to data subjects. The intention to effectively ensure an adequate level of data protection of an agreement making such a statement remains doubtful. Another critical element of the agreement is constituted by the provisions of Article 22. Accordingly, changes in domestic law with material effect on the agreement are generally permitted, only the parties must ensure sufficient notification to each other. Thus, changes substantially affecting the agreement's provisions, for instance in terms of data security measures, may be adopted legally. Given these reflections, it is noteworthy that the agreements show striking differences in the extent to which data security is factually ensured. In addition, the wording "*in particular*" is to be found throughout the agreements, for example in Article 9(5) of the EU-Canada and in Article 3(3) in the EU-Australia agreement. It indicates that subsequent obligations may not have

exclusive character. Thus, it leaves room for the inclusion of further aspects in the legal interpretation of the agreements.

4.4. Conclusion on Third Country PNR Data Transfer Agreements

Prima facie, the provisions of the external PNR agreements between the EU and third countries seem acceptable in light of ensuring a higher level of public security against the terrorist threat. Official affirmations on full respect of PNR data proceedings to EU fundamental rights, issued most commonly by the Commission, suggest that data that flows outside of the EU is protected sufficiently. Past efforts of improving data protection safeguards, primarily under the Commission's Communication on the global approach to transfers of Passenger Name Record data to third countries of 2010, reaffirm this believe. However, the analysis of the bilateral PNR agreements has shown differently. When taking a deep dive into the agreements, considerable legal gaps on privacy and data protection safeguards become evident. These, in sum, pave the way for infringements of European fundamental rights and freedoms of European citizens. In that regard, the Commission's official affirmations on the notion of external PNR data usage seem a farce. The full respect to highest data protection standards and fundamental rights which the Commission claims on, is certainly not guaranteed in full swing. The results of the analysis above indicate that especially parts of the EU-US agreement must be viewed critically. In the agreement, not only the number of legal loopholes detected is the largest but more importantly, the severity of these is by far most considerable. Moreover, reference to individual's rights is mostly related to safeguards incorporated in US law. As stated in section 2.2 of the study, US law is generally characterized by a privacy approach that provides a less strict level of data protection than the European one. Hence, the data protection standard has been diminished by benchmarking US law instead of EU law. All in all, regardless of which category is envisaged, all external PNR agreements reveal significant legal loopholes which the EU tend to conceal under superficial statements. Regarding the principles underlying PNR data transfer outside of the EU, the findings of this chapter suggest that the safeguards, praised to fully guarantee the protection of personal data in the external agreements, remain without substance. This is especially crucial considering the advocates of PNR data proceedings, putting these delicate safeguards forward as a key argument in favor of the data utilization in the law enforcement field.

5. THE CONSISTENCY OF EXTERNAL PNR DATA TRANSFERS WITH EUROPEAN DATA PROTECTION STANDARDS

5.1. Introduction to the Consistency of External PNR Data Transfers with European Data Protection Standards

Building on the findings of the subsequent chapter, this chapter studies the consistency of external PNR data transfers to third country's law enforcement authorities with the standards on privacy and data protection embedded in European legislation. For this purpose, it provides a section on significant landmark decisions of the CJEU, namely the Schrems case and Opinion 1/15 (*section 5.2*). Ultimately, the findings from the case-law analysis are utilized to extend the scope of analysis to the entirety of internal and external EU PNR legislation. This enables the chapter to conclude an answer the fourth subquestion: To what extent are external PNR data transfers for security purposes consistent with European data protection standards? (*section 5.3*).

5.2. Landmark Decisions of the CJEU on External Data Processing

In the following both cases, Schrems and Opinion 1/15 are described separately by referring to the respective problems raised. Firstly, emphasis is set on the Schrems case, which set groundbreaking obligations on the EU data protection regime in 2015 (*section 5.2.1*). Despite no direct relation to PNR, the case associated data protection concerns of mass surveillance practices conducted by US authorities and, in that line, determined the adequacy decision holding obligations on the protection of data (PNR data included) flowing outside of the EU. Secondly, Opinion 1/15 of the CJEU on the EU-Canada PNR agreement is studied (*section 5.2*.2). In 2014, the Opinion framed a precedent case to the question whether the agreements on PNR data proceedings are in line with the EU Treaties and the CFREU. In view of the broad scope of the judgment, only its key elements of interest for the study are scrutinized. Afterwards, the chapter includes a follow-up section on the interplay between the Opinion and EU PNR data practice on the internal and external level (*section 5.2.3*). The latter is determined by Directive 2016/681 and the bilateral agreements between the EU and third countries.

5.2.1. The Schrems Case

The Schrems case is named after Austrian law student and data protection activist Maximilian Schrems, who considered the data routine conducted by the social media network Facebook unlawful. Although his contract was registered within the EU under Facebook Ireland, a subsidiary of the American Facebook Incorporated, his personal data kept being transferred to US servers. In 2013, Schrems requested a confirmation on the legality of the practice in light of the adequacy principle stated in Directive 95/46/EC. The principle obliges the EU to qualify a data receiving country to provide an adequate protection for personal data of EU citizens and, thereby, constitutes one significant ground for external cross-border data transfers. Encouraged by the Snowden revelations of 2013, Schrems argued on the alleged involvement of Facebook Incorporated in US authorities' mass surveillance practices, which he considered a serious infringement of the adequacy principle. Accordingly, a sufficient level of

data protection may not be guaranteed due to American inferior practice on data security. The Irish Data Protection Commissioner (IDPC) became entrusted with the matter because Facebook Ireland has its servers located within the country. With respect to the Commission's Decision 2000/520/EC, the Safe Harbor Decision, the IDPC rejected Schrems' request as *frivolous and vexatious* (IEHC, 2014). The Safe Harbor Decision, under which many US companies, including Facebook, have operated, states that personal data transferred to US companies participating in the Safe Harbor scheme is adequately protected. In response to the findings of the IDPC, Schrems judicially reviewed the case by making explicit reference to the CFREU, especially to Articles 7 and 8 CFREU. As outlined previously, the CFREU enshrines various fundamental rights for EU citizens, including the rights to privacy (Article 7) and data protection (Article 8). Schrems based his claim on the violation of both rights, since Facebook was neither willing to adjust or erase his Facebook activity record, nor grant a general user accessibility to it. The Irish High Court referred the case to the CJEU, where the Safe Harbor Decision was invalidated in its entirety based on Schrems' CFREU related argumentation (Schrems v Data Protection Commissioner, 2015). This caused major changes in data flows from the EU to the US and led to the conclusion of a descendant agreement, the so-called EU-US Privacy Shield. With this decision, the CJEU demonstrated that it does not tolerate breaches of EU law and specifically of fundamental Human Rights in favor of an international agreement, regardless of its importance for the transatlantic relationship. Although the rights at stake, the right to respect for privacy and the right to the protection of personal data may not be absolute, the CJEU in its judgment in Schrems prohibited an international agreement to entail integral restrictions of these rights.

After a careful review of the Commission's Safe Harbor Decision, several elements were found to infringe EU fundamental rights. In the Safe Harbor scheme, there was, for example, a derogation incorporated, allowing for the processing of personal data for US national security, public interest and law enforcement requirements, irrespective of safe harbor principles (§84). The provisions of Article 25 of Directive 95/46/EC on the principles of data proceedings to third countries were crucial for the decision as they introduced a strict set of rules on external data flows. The principles not only concerned various aspects related to data proceedings, such as the nature, purpose and duration of data to be transferred, but also country specific criteria including the rule of law in force and the level of security measures provided for by the recipient (Article 25(2)). Altogether, the provisions determined whether the Commissions found a third country to ensure an adequate level of protection for EU citizen's basic rights and freedoms in the meaning of the CFREU (Article 25(3)). In the event the Commission considered the level of protection not adequate, Member States were obliged to prevent data transfers to the country in question (Article 25(4)). Since the Directive was replaced by the GDPR in May 2018, Article 45 of the new legislation forms the updated basis for the Commission's adequacy decision. In Schrems, the CJEU gave a judicial determination on the meaning of the term *adequacy* as stated in Article 25 of Directive 95/46/EC. Accordingly, a third country is not required to adopt the same data protection standard to be found within the EU (§73). Hence, the legislation of the recipient country may

differ from intra-European regulations. An adequate level of data protection is rather ensured given a third country to provide for a standard equivalent to the one afforded by Directive 95/46/EC by reason of its domestic law or its international commitments (§75). From a linguistic viewpoint, the term has been consequently attributed to the meaning of satisfactory or sufficient. Moreover, the CJEU obliged the Commission to monitor legislative changes in third countries with potential effect to the functioning of the adequacy decision (§77). This ongoing obligation shall prevent changing circumstances in the domestic legacy to jeopardize the initial assessment of the Commission and results in regular reviews on the factual level of protection in the third countries.

Although the judgment in Schrems was laid down in an economic context, since the Safe Harbor Decision concerned external data flows in the business sector, it has indeed entailed implications for data proceedings in the security field. This does also include PNR data proceedings outside of the EU governed in Directive 2016/681. With this in mind, the following implications for external PNR data flows to third countries security authorities may be identified. Firstly, the CJEU has highlighted the importance of sufficient protection standards for data that leaves the EU (§91). These standards build an active criterion PNR data transfers must comply with and, thus, require constant monitoring and review under the responsibility of the Commission. The additional obligation to frequently ensure an adequate level of data protection has already been adopted in Article 5 of the EU-Australia and EU-Canada agreement and Article 19 of the EU-US agreement. Besides, future PNR agreements will be required to provide for ongoing monitoring of the third country's data protection legislation. In addition, the CJEU explicitly acknowledged the content of electronic communications to be protected under Article 7 CFREU (§94). Thereby, it has confirmed the validity of EU fundamental rights and freedoms for electronic datasets and thus for PNR data. With regards to the external dimension of the study, it should be noted that with its judgment in Schrems, the CJEU has for the first time utilized data protection as a vehicle to expand the reach of the CFREU to cover situations involving third countries (Kuner, 2018).

5.2.2. Opinion 1/15

Next, the emphasis is shifted to Opinion 1/15 that specifically affects PNR data proceedings outside of the EU. To the present day, the Opinion is the first ruling in which the CJEU evaluated the compatibility of an international agreement according to the CFREU. It is, moreover, the only case-law with direct implications on bilateral agreements governing the external transfer of PNR data from the EU to third countries. As the case concerns the relation of EU fundamental rights and freedoms to external agreements, it holds significance for the EU's negotiation position on the international stage (Kuner, 2018). Furthermore, it is expected to have a domino effect on the EU PNR legislation in force as well as on future policies and agreements. Regarding existing legislation, the effect comprises the EU-Australia and the EU-US PNR agreement on the external dimension and Directive 2016/681 on the internal dimension. Considering this, the case is, in fact, key for the evaluation of the compliance of internal PNR data safeguards with external, cross-border PNR data transfers and, thus, for concluding a

comprehensive answer to subquestion 4. As the study has stated previously, the Parliament has, on the grounds of Article 218(11) TFEU, sought an Opinion of the CJEU concerning the compatibility of the draft agreement to primary EU law, on the one hand, and to the appropriate legal basis for the Council decision on the other hand. The Parliaments requests on the CJEU have been laid down as follows:

> 1. Is the [agreement envisaged] compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to protection of personal data?
>
> 2. Do Articles 82(1)(d) and 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the [agreement envisaged] or must that act be based on Article 16 TFEU? (CJEU, 2017).

In its Opinion on the EU-Canada draft agreement, the CJEU firstly reviewed the legal basis for the adoption of the agreement. The Parliament in its second question demanded the CJEU to determine whether the draft agreement's legal basis is constituted in notion of judicial cooperation in criminal matters and police cooperation (Articles 82(1)(d) and 87(2)(a) TFEU) or on the grounds of the fundamental right to data protection (Article 16 TFEU). The Articles in question exemplarily illustrate the European balance act between security objectives and data protection rights. Which of the two objectives is to be prioritized in terms of external PNR data proceedings? The CJEU in Opinion 1/15 does not provide an ultimate answer to this question. Rather, the argumentation recognizes, that, considering the aim and content of the envisaged agreement, it pursued two inextricably linked objectives, namely PNR data processing for fighting terrorism and other serious crimes and safeguarding the right to protection of personal data (§77). Given this exceptional case of an act pursuing two inseparably linked objectives simultaneously, the envisaged act must be constituted on various legal bases. Accordingly, the draft agreement had to be founded on both, Article 87(2)(a) TFEU with regards to security and police cooperation and Article 16 TFEU with regards to data protection (§104). Article 82(1)(d) TFEU, however, was not found to serve as appropriate legal basis because the agreement does not refer to the aim of fostering judicial cooperation in criminal matters (§102).

Secondly, regarding the first question posed by the Parliament, the CJEU addressed the combability of the draft agreement with European primary law and, in essence, with the rights to private life and protection of personal data. Although the CJEU recognized the right to data protection to be enshrined in both, Article 8 CFREU and Article 16(1) TFEU, in its evaluation, it announced to refer to Article 8 CFREU solely since it imposes the conditions under which personal data may be processed more specifically (§120). Additionally, it did not differentiate between Articles 7 and 8 CFREU throughout the Opinion, which is, nevertheless, in line with the custom of past judgments. The CJEU embarked on

the first question by considering the compatibility between the draft agreement and the rights to privacy and data protection emerging from the TFEU and the CFREU. With respect to the scope of PNR data, which covers considerable detail about individuals including sensitive information such as religious belief, the CJEU held that the systematic analysis by automated means as conditioned by the agreement does indeed entail an interference with EU fundamental rights of Articles 7 and 8 CFREU (§126). As the automated analysis of PNR data involves some margin of error, the CJEU imposed the need for a human supervisor responsible for carrying out an individual examination of any suspicious case prior to counter-actions being taken (§173). This safeguard shall prohibit automated processing leading to discrimination in the meaning of Article 21 CFREU.

Since the rights to private life and data protection are not absolute, the CJEU laid down an extensive argumentation to examine whether the interferences may be justified in confrontation with other fundamental rights. Such legal justification is obliged to specify the purpose and legal basis of the data flow and to respect the essence of the rights in question. In that vein, limitations on data protection measures are ensured to respect the principles of proportionality and necessity. Given the objective of combating terrorism and criminal offenses in order to guarantee public security, the transfer of PNR data under the agreement was considered a suitable measure to reach this goal (§151; 153). With this statement the CJEU, in substance, expressed PNR data proceedings for security objectives to be compatible with European law. This confirms the lawfulness of PNR exchange practice on a general level. Nevertheless, the CJEU in its analysis found several points of criticism that lead to the conclusion that data protection standards were not sufficiently guaranteed in the agreement's provisions and, hence, not respecting Articles 7,8 and 52(1) CFREU. The subsequent elements of the draft agreement that were subject to critical assessment by the CJEU are presented to provide a comprehensive basis for the upcoming analysis, in which the implications from case-law on additional PNR legislation, including Directive 2016/681, are studied.

In its evaluation of data protection safeguards, the CJEU criticized several provisions in the agreement. These concerned the delimitation of PNR data to be transferred (§163), the automatic analysis of the data by Canadian security authorities (§173) and the lack of precision on proceedings on case-by-case basis (§181). Thereafter, the CJEU reviewed PNR data retention based on proportionality and necessity obligations. It found that the coverage of all passengers provided for in the agreement was not unacceptably broad (§189) and that the retention period of five years did also not exceed the limits of the necessity principle (§209). However, because Canadian security authorities are not restricted in reverting retained PNR data, for example, by the requirement to seek judicial approval prior to the retrieval, the CJEU finally declared the agreement's provisions on data retention to go beyond the scope of proportionality and necessity (§208; 211). With this, it generally accepted data retention given a specific purpose, but called on the introduction of satisfactory extra safeguards. These shall further distinguish between retention and use of personal data from passengers staying on Canadian territory and from those who have left the country (§232(3)(c)(d)). This link between data retention and territorial

stay seems secondary at first sign but introduces a revolutionary approach on data retention. Subsequently, the CJEU addressed the disclosure of PNR data to government authorities. By referring to the Schrems case, it stated that third countries must ensure a level of data protection "essentially equivalent" to the standards deriving from EU law either through an independent international agreement or through a Commission's adequacy decision (§214). Given that the draft agreement allows onwards transfer of PNR data on both national and international level, the draft agreements provisions on data disclosure were considered too broad according to the necessity principle (§215). Therefore, the onwards transfer of PNR data is required to be limited in that sense. Further, passengers were assigned with a set of rights, including the right to data rectification and the right to notification in the event of their personal data being used by a security authority (§220; 223). Because these shall apply regardless of threats to an ongoing investigation, the CJEU clearly pursued its evaluation in favor of data protection. Finally, the CJEU held that the envisaged agreement fails to appoint an independent authority responsible for monitoring compliance with security safeguards in the meaning of Article 8(3) CFREU (§231). This finding provided further evidence on the lack of combability between the agreement and data protection standards emerging from the European rule of law.

While the envisaged agreement has not per se been invalidated due to the wrong legal basis, the finding of the CJEU on the above-mentioned substantive elements did. In its argumentation the CJEU in conclusive manner evoked that a high level of protection is required when data is transferred outside of the EU. Thereby it followed the line of previous judgments in the field, including Digital Rights Ireland and Schrems, which were referred to at several points throughout the evaluation. In comparison to these previous judgments, in Opinion 1/15 the CJEU laid down a more detailed set of requirements for the protection of individual's personal data to be transferred outside of the EU. Despite the lack of comment on the systematic transfer of large amounts of PNR data and, in connection, the reservations on mass surveillance, the CJEU did demonstrate the significance of respect to privacy and data protection deriving from the Treaties and the CFREU and imposed the European standard of data protection externally on international agreements. However, for third countries seeking the conclusion of a PNR agreement with the EU, the judgment results in great legal uncertainty. Considering the resources Canadian negotiators have invested in the now invalided agreement, the EU is also likely to appear an unreliable contradicting partner on the international level.

5.2.3. Implications on PNR Data Processing Emerging from Opinion 1/15

Albeit general data protection guidelines have emerged from the Schrems case, Opinion 1/15 precisely laid down lacks on the level of data protection in the EU-Canada PNR agreement. Thereby, not only the decision has invalidated the envisaged agreement itself but also various indirect implications for the standard of data protection have emerged for EU PNR data practice, both internally and externally. By adopting the EU internal dimension, this section begins with a brief elaboration of the interplay of Opinion 1/15 and the European PNR Directive. In fact, the CJEU in its Opinion directly referred to the Directive at several points, for instance, in relation to the collection of sensitive data under PNR

processing (§166). Moreover, when reconsidering the provisions of Directive 2016/681 (*section 3.2*), one may find that it already includes safeguards that were required for the envisaged EU-Canada agreement to ensure combability with EU fundamental rights. For instance, Article 6(5) of Directive 2016/681 on human intervention on PNR data proceedings in conjunction with paragraph 232(3)(b) requires clarification on PNR data analysis by automated means. Hence, the above-mentioned points of criticism on safeguards in the EU-Canada agreement (§173; §181; 208-211) are already adopted sufficiently in the EU PNR Directive. In response to this point, the CJEU made in paragraph 181 of the agreement, a specification of the scope of proceedings on a case-by-case basis is given in Article 6(2)(b). Furthermore, considering the requirement to define conditions underlying the reversion of retained PNR data and, consequently, the incompliance to the principles of proportionality and necessity (§208-211), Article 12(3) of the Directive includes a set of provisions under which data reversion is permitted. Thereby, Article 12(3)(a) recognizes respect to the necessity principle, whereas Article 12(3)(b) obligates judicial approval prior to the data being reverted. These examples provide evidence that the EU internal PNR Directive served as a model for the CJEU in formulating corrective protection safeguards to the EU-Canada draft agreement. Despite approving the data protection safeguards of Directive 2016/681 sufficient, the CJEU in its evaluation provided some veiled points of criticism towards the PNR Directive. The legislation does not include, for instance, any right of notification in the event of PNR data usage by security authorities as derived from Opinion 1/15 (§220; 223). Moreover, the link between data retention and territorial stay (§232(3)(c)(d)) may have considerable repercussions on the Directive, since it does not distinguish between individuals staying in the EU and those who have left. The adoption of such a distinction in EU internal legislation would entail severe challenges in practice, since PNR data analysis were required to function on grounds of an Entry-Exit System similar to the American one. All in all, the additional protection safeguards on PNR data proceedings, as issued by the CJEU, are most likely to be carefully considered by EU policy-makers and, thus, mark a challenge to the current form of Directive 2016/681 in the context of upcoming policy reviews.

Next, the impact of Opinion 1/15 on the external dimension of PNR data legislation, comprising the bilateral agreements between the EU and third countries on PNR data transfer, is analyzed. In the first place, emphasis is shifted on the legal basis of the EU-Canada agreement that was declared wrong by the CJEU. Since all PNR agreements between the EU and third countries are underlying Articles 82(1)(d) and 87(2)(a) TFEU, the two other agreements suffer the same legal basis dilemma. More importantly in light of concluding an answer to on the fourth subquestion in the subsequent conclusion of this chapter, are the implications on consistency of external PNR data transfers with EU data protection standards. The CJEU itself did not comment on the compliance of the additional third country PNR agreements with EU fundamental rights. Reconsidering that in chapter 4 the agreements were found to be very similar in terms of content and structure, the major rights infringements to privacy and data protection become, however, also evident in the EU-US and EU-Australia agreement. Although the CJEU has confirmed the violation of rights on the example of the EU-Canada draft agreement, it

indirectly confirmed the two other agreements to not fully respect privacy and data protection as well. Therefore, the points of criticism are applicable to the entirety of EU external PNR legislation. For example, neither the EU-US nor the EU-Australia agreement species the circumstances determining case-by-case proceedings of PNR data. Significant analogies between the agreement's provisions are also visible in terms of data retention, onwards transfer and data disclosure, in general and with regards to sensitive data, and data transfer and analysis by automated means. Moreover, the analysis in chapter 4 has shown how parts of the EU-US agreement stand out from the entirety of third country PNR agreements, however in negative sense. Legal gaps on EU data protection standards are most distinct in the agreement at hand. Given this, one may assume the scope of its rights infringements to expand beyond the findings of Opinion 1/15 under judicial review. However, according to the provisions of Article 263(6) TFEU, such review is not possible anymore because the agreements are in force for too long.

5.3. Conclusion on the Consistency of External PNR Data Transfers with European Data Protection Standards

This chapter aimed to examine to what extent external PNR data transfers in the security field are consistent with European standards of the protection of personal data. To approach the question, the judgment of the CJEU in the Schrems case was analyzed firstly. Although the case revealed rather indirect implications for external PNR data practice, it was found that these have indeed been adopted in the bilateral PNR agreements between the EU and third countries. It was shown, that the obligation to ensure frequent monitoring of third countries data protection legislation as established by the CJEU, has been fully adopted in all PNR agreements. The subsequent analysis of Opinion 1/15 has, however, revealed various points that the CJEU in its evaluation of the EU-Canada PNR agreement has recognized to violate European standards on data protection as determined in the CFREU and the Treaties. Based on the argumentation on the invalidated EU-Canada agreement, the study reasons that the additional PNR agreements with the US and Australia must be infringing EU citizen's rights likewise. This inference results from the agreements having unveiled distinctive analogies in chapter 4. Based on the analysis of the CJEU's findings in Opinion 1/15, the chapter showed that the transfer of PNR data to third countries is not fully in line with EU standards. Thereby, reference was made to the points which limit the level of consistency between external PNR data transfers and European data protection standards.

Section 5.2.2 has in detail outlined the envisaged agreement's provisions from which discrepancies arise. The elements concern not only criticism on data protection safeguards of the agreement, that the EU provides for the data, but also requirements with revolutionary character that have not been established in PNR data practice (internally or externally) yet. Therefore, attention must be paid to the extent the European legislative framework itself respects the obligations imposed by the CJEU. Since Opinion 1/15 has, by linking data retention and territorial stay (§232), in fact, established new safeguards on PNR data practice, the EU PNR Directive requires corresponding adaptions. Given this, consequences

deriving from the Opinion will concern the entire European PNR legislation within the EU. Nevertheless, in the context of evaluating data protection safeguards of the EU-Canada agreement, the CJEU has assimilated its criticism according to the provisions of Directive 2016/681. This confirms the EU PNR Directive to include sufficient data protection safeguards in substance. With respect to the public controversy on PNR data usage as addressed in section 3.3, the CJEU in Opinion 1/15 did rather rebutted than confirmed the points of criticism stated in the discourse. It reaffirmed, for example, the necessity of a five-year data retention period (§209), which is often criticized as too long. Moreover, the CJEU juridically rejected PNR data practice to equal mass-surveillance by confirming the lawfulness of PNR data exchanges on a general level (§151; §153).

Altogether, in Opinion 1/15, the CJEU has demonstrated a new line on the significance of data protection compliance in its past judgments. After Digital Rights Ireland and Schrems, Opinion 1/15 constitutes the preliminary milestone in addressing legal challenges on the rights to privacy and data protection arising from increasing data flows in the digital age. In this context, Kuner notes that the CJEU in its judgment "takes the standards that [it] applied to data protection in other key judgments […] and applies them to international agreements." (Kuner, 2018). Given the analysis of implications in section 5.2.3, it is noteworthy that consequences from the judgement will concern the entire PNR legislation within the EU. According to the parameters on PNR data practice determined in the CJEU judgment, large-scale adoptions must follow in order to proceed towards greater consistency of external PNR data transfers with domestic data protection standards of the EU.

6. CONCLUSION ON THE BALANCE BETWEEN SECURITY OBJECTIVES AND THE PROTECTION TO PERSONAL DATA WITHIN THE EU

With the rise of new forms of threats to public security, primarily of terrorist nature, international police and law enforcement authorities have increasingly realized the potential of PNR data in countering the risk of violent incidents. In Chapter 2 of this study, it was found that the EU in line with the essence of privacy rights as fundamental rights, has emphasized special protection features on the data of EU citizens. In order to maintain these standards in the context of external data transfers, legal conditions on the required level of protection in third countries have been explicitly formulated within the EU. The study has shown, how these standards have been determined not only through the adoption of precise laws and policies, but also within case-law. In the security field, data is further conditioned to have a pre-determined purpose underlying the transfer to which all further proceedings must comply. Introducing the by the case-study, Chapter 3 examined the European approach on PNR data. With its entry into force in May 2018, Directive 2016/681 closed a significant legal gap by constituting the first EU PNR policy. The legislation was, in sum, considered to establish comprehensive data protection safeguards. Shifting emphasis to the external dimension of the study, cross-border PNR data flows were stressed in Chapter 4. The analysis of the bilateral agreements between the EU and third countries on PNR data transfers in the security field revealed significant shortcomings regarding protection safeguards that secure privacy and data protection rights within the European legislative framework. Chapter 5 subsequently studied the consistency between external PNR data flows and European data protection standards. The analysis of relevant case-law allowed the study, in this context, to draw implications on the respective bilateral PNR agreements assigned to these European standards. It was found, that external PNR data transfers in the security field governed by the agreements do not fully comply with the level of data protection guaranteed within the EU. Considering the findings of the previous chapters, an answer to the initial research question can be provided in the following. The study's main research was: To what extent do European data protection standards enable external data proceedings in the fight against terrorism and serious crime whilst safeguarding personal data of European citizens?

The study has outlined how personal data is transferred and proceeded outside of the EU regardless of clear restrictions on the rights to privacy and data protection as fundamental Human Rights. Therefore, it can be stated that European data protection standards do not constitute an obstacle for the utilization of data-related security instruments in international law enforcement cooperation. Apparently, the EU holds its standards, in terms of respect to privacy and protection of personal data, on such a high level, it is not able to successfully ensure compliance with them in the context of anti-terrorism synergy with external partners. The lack of data protection safeguards in the bilateral PNR agreements vividly illustrate this inability. Under the purpose of fighting terrorism and serious crime, the EU accepts the conclusion of international agreements with third countries that go beyond the internal obligations of Human Rights protection. In confrontation with persistent concerns on this procedure, the EU has made

attempts to adopt improved protection safeguards for the external dimension of such cooperation, suggesting intentions of the EU to ensure respect to the protection of personal data. However, the protection standards within the EU do not intrinsically inhibit the transfer of data for security cooperation. Rather, the strategic partners of the EU, most notably the US, have resisted the diffusion of EU law beyond its borders and thus prevented the EU from upholding its domestic level of privacy and data protection in the international sphere. This suggest an asymmetry within the countries relationship, that has been observed by many scholars before (Argomaniz, 2009; Loewe 2016). In fact, global standards on data protection in the security field appear to be under US interference (Blasi-Casagran, 2017), making it difficult for the EU to uphold its fundamental values in this area, especially under the presence of differences in the character of domestic data protection regimes that has been examined in section 2.4. The current line of the CJEU on privacy and data protection does in this regard indicate a paradigm shift in the direction of a more symmetry between the EU and the US.

With regards to the balance between security objectives and privacy and data protection as fundamental Human Rights, the study has provided evidence that, to date, security objectives still determine the course of external data sharing in law enforcement cooperation. The example of PNR data transfers has illustrated the difficult progress of the EU towards combining the promotion of effective counter-terrorism measures in liaison with compliance to the right to data protection as a fundamental Human Right. Reconsidering that section 2.3.3 on the European approach on counter-terrorism has emphasized the importance of collaboration with international partners for the effective combat against terrorism, the EU holds a vested interest in cross-border information exchange. Because of this strategic value of international cooperation in fighting terrorism and serious crime, the security interest is more likely to take over. This results in the EU to accept cooperative measures infringing fundamental Human Rights. However, it is not the cross-border transfer of data that *per se* constitutes a violation to the rights to privacy and data protection. The challenge rather lies in the data practice prevalent in third countries receiving the data. As the analysis of the bilateral PNR agreements in Chapter 4 and of Opinion 1/15 in Chapter 5 has shown, the European dilemma is a result of third countries holding on to their respective approach on data protection, according to the prioritization of security objectives.

Since from a European point of view, it is equally important to ensure the protection of citizen's rights as well as maintaining a general level of public safety, future agreements on bilateral data exchanges in the law enforcement sector will be required to assign even greater emphasis on the protection of personal data. To advance towards external safeguards that guarantee a privacy standard similar to the European one, the evaluation stated within Opinion 1/15 provides particular guidance. Especially in relation to the evaluation of data protection safeguards, in which the CJEU criticized several provisions of the EU-Canada agreement, (section 5.2.2), links to Directive 2016/681 as European internal PNR legislation constituted a benchmark for the sufficient level of protection of individual's personal data. In general, the emphasis on elements requiring revision within the international agreements will entail a large number of adaptions. The scope of these adoptions will range from renegotiations of the invalidated

draft agreement with Canada on the grounds of the Opinion, to revisions of the EU-US and EU-Australia agreements in the upcoming years. In addition, negotiations on future PNR agreements with third countries, for example with Mexico, will also be affected by Opinion 1/15. Although the actual effect remains to be seen during the progress of PNR policy reviewing, the results are expected to provide stricter data protection provisions, not just on paper but chiefly with effect on PNR data practice. In any case, European negotiators are implied to enforce several amendments to the agreements. In order to ensure the lawfulness of external PNR data transfers, the safeguards imposed by the CJEU must be enforced while simultaneously upholding EU data protection principles of the CFREU and the Treaties. This assigns the EU with the opportunity to affirm its domestic data protection principles on the international scale within the revisions of the agreements. Depending on how well the EU bargains on factually effective data security safeguards during the upcoming negotiations, the future agreements may ultimately provide for better protection of EU citizen's PNR data.

Applying consistent protection standards internationally might involve the design of a single model PNR agreement, instead of adherence to individual agreements with strategic partners. In such a model agreement, the EU may stress its position on the rights to privacy and data protection by precisely defining a complete set of rules and obligations to be safeguarded in PNR data practice. Considering the Commission's intentions to enhance PNR data exchanges with additional third countries, the implementation of such a model agreement is expedient especially in the long term. The model agreement would set out requirements the contracting party must meet for receiving PNR data from EU citizens and in this line determine precise standards for the external data exchanges in the security field. Noting that in 2004 Asinari and Poullet referred to PNR data transfers as "no man's land story" (Asinari & Poullet, 2004), the EU has made major progress since that time. It is to hope that the development will not come to an end until the data travels with the same safeguards assigned for it in EU law.

BIBLIOGRAPHY

Literature

Books

Blasi-Casagran, C. (2017). *Global data protection in the field of law enforcement: An EU perspective*. Routledge New York.

Journals

Asinari, M. V. P. & Poullet, Y. (2004). *Public security versus data protection: Airline passengers' data: adoption of an adequacy decision by the European Commission. How will the story end?*. Computer Law & Security Report, 20 (5), 370-376.

Balzacq, T. (2008). *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies*. Journal of Common Market Studies, 46 (1), 75-100.

Bakker, E. (2015). *EU Counter-radicalization Policies: A Comprehensive and Consistent Approach*?. Intelligence and National Security, 30 (2-3), 281-305.

Bures, O. (2007). *EU Counterterrorism Policy: A Paper Tiger?*. Terrorism and Political Violence, 18 (1), 57-78.

Chirlesan, G. (2015). *European security and the terrorist threat: Evolutions and current ways of managing it*. International Conference knowledge-based organization, 21 (1), 21-27.

Coolsaet, R. (2010). *EU counterterrorism strategy: value added or chimera?*. International Affairs, 86 (4), 857-873.

Dumitriu, E. (2004). *The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism*. German Law Journal, 5 (5), 585-602.

Dimitrova, A. & Brkan, M. (2018). *Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair*. Journal of Common Market Studies, 56 (4), 751–767.

Edwards, G. & Meyer, C. O. (2008). *Introduction: Charting a Contested Transformation*. Journal of Common Market Studies, 46 (1), 1-25.

Golino, L. R. (2002). *Europe, the war on terrorism and the EU's international role*. The Brown Journal of World Affairs, 8 (2), 61-72.

Argomaniz, J. (2009). *When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms*. Journal of European Integration 31(1), 119-136.

Kaunert, C. & Occhipinti, J. D. & Léonard, S. (2014). *Introduction: supranational governance in the Area of Freedom, Security and Justice after the Stockholm Programme*. Cambridge Review of International Affairs, 27 (1), 39-47.

Kuner, C. (2018). *Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*. Common Market Law Review, 55 (3), 857–882.

Léonard, S. (2010). *The Use and Effectiveness of Migration Controls as a Counterterrorism Instrument in the European Union*. Central European Journal of International and Security Studies, 4 (1), 32-50.

Loewe, D. (2016). *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?*. International Criminal Law Review, 16 (5), 856-884.

McDermott, Y. (2017). *Conceptualising the right to data protection in an era of Big Data.* Big Data & Society, 4 (1), 205395171668699.

Papakonstantinou, V. & de Hert, P. (2009*). The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on Either Side of the Atlantic*. Common Market Law Review 46 (1), 885-919.

Potemkina, O. (2017). *Terrorism threat in Europe: The European Union's response.* Contemporary Europe, 3 (1), 17-27.

Taylor, M. (2015). *Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement*. Spanish Yearbook of International Law, 19 (1), 221 – 234.

Wittendorp, S. (2016). *Conducting Government: Governmentality, Monitoring and EU Counter Terrorism.* Global Society, 30 (3), 465-483.

Policy Documents

Article 29 Working Party (2013). *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203.

Article 29 Working Party (2010). *Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, 622/10/EN WP 178.

Article 29 Working Party (1999). *Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights*, 5143 /99/EN WP 26.

Bigo, D. & Brouwer, E. & Sergio C. & Sergio C. & Guild, E. & Guittet, E. & Jeandesboz, J. & Ragazzi, F. & Scherrer, A. (2015). *The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda.*

Brouwer, E. (2011). *Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers.*

Council of the European Union (2005). *The European Union's strategic commitment: To combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live in an area of freedom, security and justice.*

European Commission (2017c). *Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security.*

European Commission (2016a). *Factsheet: How will the data protection reform help fight international crime?*.

European Commission (2016b). *Transatlantic Data Flows: Restoring Trust through Strong Safeguards*.

European Commission (2015). *Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement"*.

European Commission (2010). *Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries*.

European Digital Rights & Panoptykon Foundation &Access (2015). *Analysis of the LIBE draft report proposal.*

European Parliament (2015a). *Towards a new European Agenda on Security*.

European Parliament (2015b). *The proposed EU passenger name records (PNR) directive: Revived in the new security context.*

European Union Agency for Fundamental Rights (2010). *Data Protection in the European Union: the role of National Data Protection Authorities.*

Information Commissioner's Office (2015). *Data Protection Rights: What the public want and what the public want from Data Protection Authorities.*

Matera, C. (2016). *Writing a bachelor thesis in law in the EPA program at the University of Twente*.

North Atlantic Treaty Organization (2014). *NATO Glossary of Terms and Definitions*, AAP-06.

Privacy International (n.d.). *Privacy and Human Rights: An International Survey of Privacy Laws and Practice.*

World Bank (2018). *International data flows and privacy: the conflict and its resolution*. Policy Research Working Paper No. WPS 8431.

Internet Sources

Arthur Cox (2017). *Group Briefing: High Court refers Schrems II case to European Court of Justice: The implications for International Data Transfers*. Retrieved from: http://www.arthurcox.com/wp-content/uploads/2017/10/High-Court-refers-Schrems-II-case-to-European-Court-of-Justice.pdf.

Arthur Cox (2016). *Group Briefing: Data Protection Update – New Legislation*. Retrieved from: http://www.arthurcox.com/wp-content/uploads/2016/05/Data-Protection-Update-New-Legislation-May-2016-WEB.pdf.

Article 29 Data Protection Working Party (2015). *Subject: Letter on EU PNR.* Retrieved from: http://www.statewatch.org/news/2015/mar/eu-pnr-letter-art-29-wp-to-chair-libe.pdf.

Coudert, F. (2016). *The Directive for data protection in the police and justice sectors: towards better data protection?*. Retrieved from: https://www.law.kuleuven.be/citip/blog/the-directive-for-data-protection-in-the-police-and-justice-sectors-towards-better-data-protection/.

Council of the European Union (2017). *Regulating the use of passenger name record (PNR) data*. Retrieved from: http://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/.

Council of the European Union (2016). *Council adopts EU Passenger Name Record (PNR) directive*. Retrieved from: http://www.consilium.europa.eu/en/press/press-releases/2016/04/21/council-adopts-eu-pnr-directive/.

Council of the European Union (2015). *"Paris Declaration" of 11 January 2015*. Retrieved from: http://data.consilium.europa.eu/doc/document/ST-5322-2015-INIT/en/pdf.

Centre Virtuel de la Connaissance de l'Europe (2007). *Gijs de Vries: "The fight against terrorism must be conducted in accordance with the rule of law"' from Le Monde (17 February 2007)*. Retrieved

from:
http://www.cvce.eu/en/obj/gijs_de_vries_the_fight_against_terrorism_must_be_conducted_in_accordance_with_the_rule_of_law_from_le_monde_17_february_2007-en-cf8989fc-de21- 4a7d-9be5-e242d9b9da40.html.

Di Francesco Maesa, C. (2016). *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*. Retrieved from: http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/?print=pdf.

European Commission (2018a). *Data Protection in the EU*. Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

European Commission (2018b). *Security Union: New rules on EU Passenger Name Record data*. Retrieved from: https://ec.europa.eu/home-affairs/news/security-union-new-rules-eu-passenger-name-record-data_en.

European Commission (2017a). *Questions and Answers: Data protection reform package*. Retrieved from: http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm.

European Commission (2017b). *Security Union: Commission presents new measures to better protect EU citizens*. Retrieved from: http://europa.eu/rapid/press-release_IP-17-3947_en.htm.

Commission (n.d.). *Transfer of air passenger name record data and terrorist finance tracking programme*. Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en.

European Council (2018). *The directive on protecting personal data processed for the purpose of criminal law enforcement*. Retrieved from: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/.

European Criminal Law Academic Network (2016). *Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. Retrieved from: http://eclan.eu/en/eu-legislatory/directive-eu-2016-681-of-the-european-parliament-and-of-the-council-of-27-april-2016-on-the-use-of-passenger-name-record-pnr-data-for-the-prevention-detection-investigation-and-prosecution-of-terrorist-offences-and-serious-crime.

European Data Protection Supervisor (n.d.). *Transparency*. Retrieved from: https://edps.europa.eu/data-protection/our-work/subjects/transparency_en.

European Data Protection Supervisor (n.d.). *Data Protection*. Retrieved from: https://edps.europa.eu/data-protection_en.

European External Action Service (2016). *Counter-terrorism*. Retrieved from: https://eeas.europa.eu/headquarters/headquarters-homepage/411/counter-terrorism_en.

Knight, A. (2016). *New Air Passenger Data Processing Rules to Apply from 2018.* Retrieved from: https://peepbeep.wordpress.com/2016/05/19/new-rules-around-the-processing-of-passenger-travel-records-in-respect-of-flights-into-or-out-of-the-eu-to-apply-from-2018/.

Loewe, D. (2016). *Time to Re-Introduce a Directive on the use of Passenger Name Record Data*. Retrieved from: http://researchonline.ljmu.ac.uk/3367/.

Vavoula, N. (2016). *'I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive.* Retrieved from: https://free-group.eu/2016/10/27/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/.

White & Case (2017). *Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation.* Retrieved from: https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation.

Legislation

Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record, 2013/0250.

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, 12.07.2012. L 186/4.

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, 11.08.2012. L 215/5.

Aviation and Transportation Security Act of 2001, Public Law 107–71—Nov. 19, 2001 (codified at 49 U.S.C. 44909(c)(3)).

Charta of Fundamental Rights of the European Union 2000/C364/01. Official Journal of the European Communities.

Council of Europe (1981). Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data (CETS No. 108).

Council of Europe (1950). European Convention of Human Rights.

Council of the European Union (2002). Council Framework Decision of 13 June 2002 on combating terrorism.

Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

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).

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 (Law Enforcement Directive).

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive).

Treaty on European Union, Official Journal C326, 26/10/2012.

Treaty on the Functioning of the European Union, Official Journal C326, 26/10/2012.

United Nations (1948). Universal Declaration of Human Rights.

Case Law

CJEU, Case C-1/15, Opinion of the Court of 26 July 2017.

CJEU, Case C-145/09, Judgment of the Court of 23 November 2010, Land of Baden-Württemberg v. Panagiotis Tsakouridis.

CJEU, Case C-362/14, Judgment of the Court of 6 October 2015, Maximillian Schrems v. Data Protection Commissioner.

CJEU, Case C-524/ 06, Judgment of the Court of 16 December 2008, Heinz Huber v. Bundesrepublik Deutschland.

CJEU, Joined Cases C-293/12 and C-594/12, Judgment of the Court of 8 April 2014, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others; Kärntner Landesregierung v Seitlinger, Tschohl and Others.

CJEU, Joined Cases C-317/04 and C-318/04, Judgment of the Court of 30 May 2006, European Parliament v. Council of the European Union; European Parliament v. Commission of the European Communities.

The High Court (IEHC), Schrems v. Data Protection Commissioner, 2013 765 JR of 2014.

ANNEX – I

1 PNR record locator code
2 Date of reservation/issue of ticket
3 Date(s) of intended travel
4 Name(s)
5 Available frequent flier and benefit information (i.e. free tickets, upgrades, etc)
6 Other names on PNR, including number of travellers on PNR
7 All available contact information (including originator of reservation)
8 All available payment/billing information (e.g. credit card number)
9 Travel itinerary for specific PNR
10 Travel agency/travel agent
11 Code share information
12 Split/divided information (e.g. when one PNR contains a reference to another PNR)
13 Travel status of passenger (including confirmations and check-in status)
14 Ticketing information, including ticket number, one-way tickets and automated ticket fare quote
15 All baggage information
16 Seat information, including seat number
17 General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information
18 Any collected Advance Passenger Information (API)
19 All historical changes to the PNR listed under points 1 to 18

I. *List of categories covered under PNR data (Blasi-Casagran, 2017, p. 96)*