University of Twente

European Public Administration

Faculty of Behavioral, Management and Social Sciences

First Supervisor: Dr. Claudio Matera

Second Supervisor Dr. Martin Rosema

BACHELOR THESIS

Intelligence Sharing Practices in the Counter Terrorism Framework of the European Union and their Implications for Individual Privacy Rights

Yannic Blaschke

s1734717

July 5, 2017

Word Count: 25.094

Key words: Counter-Terrorism, Intelligence Exchange, Fundamental Rights, Privacy, Data Protection, Europol, Intelligence Analysis Centre

ABSTRACT

The challenge of international terrorism has progressively increased the willingness of Member States of the European Union to engage in the exchange of intelligence to prevent and investigate terrorist attacks. Yet, the exchange of personal data needs to be carefully balanced with the Union's constitutional values and fundamental rights. To answer the research question '*To what extent does the existing EU regulatory framework on the sharing of intelligence information for countering terrorism respect the rights of individuals?',* this study therefore provides an analysis of the extent to which the European Union's standard of protection concerning the fundamental rights of privacy and data protection are safeguarded in the regulatory frameworks and intelligence exchange actions of the most relevant Union counter terrorism actors and agreements. It does so by evaluating relevant legislation in the light of available documents concerning the conduct of the actors' respective counter terrorism information exchanges. The study comes to the conclusion that the level of protection in counter-terrorist intelligence exchanges of the Union is not universal and is dependent on the level of integration of the environment in which counter-terrorist actors operate.

ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CTG	Counter Terrorism Group
DHS	Department of Homeland Security
DPO	Data Protection Officer
EuroDac	European Dactyloscopy
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECTS	European Counter Terrorism Centre
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EFTA	European Free Trade Area
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
EIS	Europol Information System
FP	Focal Point
FIU	Financial Intelligence Unit
FDCT	Framework Decisions on Combating Terrorism
GCHQ	Government Communications Headquarters
INTCEN	EU Intelligence Analysis Centre
INTDIV	Intelligence Division
NATO	North Atlantic Treaty Organisation
PNR	Passenger Name Records
SIAC	Single Intelligence Analysis Capacity
SIS	Schengen Information System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program

CONTENTS

1. INTRODUCTION

12 years after Gijs de Vries, former EU coordinator for counterterrorism summarised that: '*You can't get closer to the heart of national sovereignty than national security and intelligence services*', his statement still holds true. The collection and use of sensitive information remains one of the core competences of the EU member states and is subject only to their individual scrutiny. However, the enormous challenges raised in terms of internal security by the threat of terrorism have led to a notable increase in the willingness to engage in the exchange of counter terrorism intelligence within the Union[1]. Most visibly, this cooperation is manifested in the institutions of the EU Intelligence Analysis Centre (INTCEN) and the newly founded European Counter Terrorism Centre (ECTC), which are, however, merely the front line of involved actors in the securitised policy arena of counter terrorism. Institutions that have formerly not been involved with counter terrorism policies have been given capacities to obtain and share counter terrorism intelligence provided by Member States in an environment in which the distinction between internal and external as well as military and civil security has become increasingly blurred.[2]

While there is little doubt that the development of EU capacities intelligence capacities is still at an initial stage and the institutions built for said purpose are technically Fusion Centers[3] in the image of intelligence merging cells of the United States rather than the 'European FBI' that some voices have been calling for, significant progress has been made in recent years and further a increase in intelligence exchanges is likely to develop in the future. The EU counter terrorism strategy of 2014 for instance specifically calls for the improvement of cross-border information exchanges, including criminal records.[4] Similarly, the EU Global Strategy adopted in June 2016 explicitly mentions the encouragement of '*greater information sharing and intelligence cooperation among Member States and EU agencies*'[5] and responses to newly arising challenges such as hybrid threats are increasingly incorporating intelligence exchange as a vital component.[6]

---

[1] J. Argomaniz, O. Bures, and C. Kaunert, 'A Decade of Eu Counter-Terrorism and Intelligence: A Critical Assessment,' 30 *Intelligence and National Security* 2015,191-206.

[2] M. D. Boer, 'Counter-Terrorism, Security and Intelligence in the Eu: Governance Challenges for Collection, Exchange and Analysis,' 30 *Intelligence and National Security* 2015,402-419.

[3] For a definition and analysis of Fusion Centers, see D. L. Carter and J. G. Carter, 'The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement,' 36 *Criminal Justice and Behavior* 2009,1323-1339.

[4] Council of the European Union, 'Report on the implementation of the EU Counter-Terrorism Strategy' (November 2014), available at: http://data.consilium.europa.eu/doc/document/ST-15799-2014-INIT/en/pdf

[5] EU global strategy on foreign and security policy, available at: <http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf >

[6] In their Joint communication to the European Parliament and the Council, the first institutional reaction proposed by the Commission is the establishment of an 'EU Hybrid Fusion Cell' within the INTCEN structures. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

Such exchanges are certainly an important integration step in a borderless Union whose security still relies on a fractured system of national law enforcement and intelligence agencies. Their vital importance for the prevention of terrorist attacks has been underscored by a variety of tragic events in which better coordination might have saved civilian lives, the most recent example being an attack in London that was carried out amongst others by an Italian whose data had been forwarded by Italian authorities, but not been used by British law enforcement.[7]

Yet, they also pose new challenges for the legal system of the EU, primarily regarding the standard of data protection that is applied in the exchange of information. Furthermore, the 2013 NSA scandal raised public awareness not only about the massive scope of intrusive capacities that intelligence agencies have in the information age, but also about the fact that EU member states agencies, above all the United Kingdoms' Government Communications Headquarters (GCHQ), have been engaged in surveillance practices that were equally questionable as their North-American counterparts.[8] These scandals reintroduced with astonishing clarity that the purposes and scale of intelligence collected by nation states can have far reaching consequences for individual democratic rights and that they need to be constantly assessed in regard to their compatibility with such fundamental freedoms.[9] While Union law cannot be applied to the collected information within the member states themselves, the information becomes part of the EU legal order as soon as it is exchanged through EU institutions, raising the question on what safeguards and mechanisms do exist to prevent intelligence that does not comply with EU human rights and data protection standards to be exchanged. This question is particularly relevant in the framework of counter terrorism, which is perceived with a fair amount of scepticism due to a variety of illiberal tendencies. It has been pointed out that there is a shift in Union counter terrorism law towards more pre-emptive measures, which regards the European population as a potential suspect, making it subject of surveillance and rendering citizens as an object of control through the logic of the 'war on terror'.[10]

1.1. THE CONTEXT OF EU COUNTER TERRORISM INTELLIGENCE EXCHANGE

Intelligence can be defined as the 'collection and analysis of open, publicly available and secret information with the goal of reducing policy-makers' uncertainty about a security policy

[7] E. McKirdy and A. Dewan, 'UK police face questions as third London attacker named', *CNN International Edition*, (London, 6 June 2017), available at: http://edition.cnn.com/2017/06/06/europe/london-terror-attack/index.html
[8] An extensive analysis of Member states individual practices can be found in D. Bigo et al., 'Mass Surveillance of Personal Data by Eu Member States and Its Compatibility with Eu Law,' 61 *Liberty and Security in Europe* 2013
[9] Cf. section 1.1.1 in ibid.
[10] Cf. Murphy in Chapter 10 of C. Murphy and D. Acosta Arcarazo, *Eu Security and Justice Law : After Lisbon and Stockholm* (Oxford: Hart Publishing 2014).

problem'.[11] The framing of the exchange of such products as a vital component in the fight against terrorism is rather recent and has developed along the general emergence of EU counter terrorist action. As analysed by Argomaniz, the development of the EU as a visible actor in the realm of counterterrorism did not begin up until after the *critical junctures* of the terror attacks of 9/11in the United States and the Madrid Train bombings of 2004. Cooperation among Member States was in the beginning concentrated in the former Third Pillar of Justice and Home Affairs, but later also spread into the framework of the Common Foreign and Security Policy (CFSP).[12] Regarding the current situation, Argomaniz, Bures and Kaunert note that there is a wide variety of EU agencies and institutions involved in counter terrorism issues, and that, except for the Counter Terrorism Coordinator, none of them is tasked solely with counter terrorism.[13] While it must be added that with 2016 we saw the establishment of the first EU counter terrorism only unit with the European Counter Terrorism Centre (ECTC), their analysis that many legal instruments used in the counter terrorism context are general anti-crime measures still mostly holds true. Concerning the nature of European Counter Terrorism law, Hamilton argues that there is an increasing securitization ongoing in what she calls an emerging paradigm of preventive justice.[14] She sees a threat for fundamental rights in the broadened scope of the framework decision on combating terrorism of 2008 and observes spill over effects of counter terrorism legislation into the 'ordinary' criminal justice sphere.[15] Murphy expresses concern that the diffuse nature of power at European level will provoke less public scrutiny on illiberal counter terrorism action and suffices that in general that the development of a new system of security in the middle of a 'war' is not ideal.[16]

It becomes clear that the European Counter Terrorism framework is a large array of political and regulatory measures whose associated actors have mostly no original relationship with counter terrorism, yet whose adopted measures have far reaching implications for the rights of citizens. Therefore, special scrutiny has to be exercised by the scientific community, including the evaluation of intelligence cooperation. Such evaluation needs to balance the acknowledgement of the peculiarities of intelligence action, in which a certain degree of secrecy is unavoidable, with the challenges such action can raise regarding democratic accountability,

[11] J. I. Walsh, 'Intelligence-Sharing in the European Union: Institutions Are Not Enough*,' 44 *JCMS: Journal of Common Market Studies* 2006,625-643.
[12] J. Argomaniz, 'Post-9/11 Institutionalisation of European Union Counter-Terrorism: Emergence, Acceleration and Inertia,' 18 *European Security* 2009,151-172.
[13] J. Argomaniz, O. Bures, and C. Kaunert, *supra* note 1
[14] C. Hamilton, 'The European Union: Sword or Shield? Comparing Counterterrorism Law in the Eu and the USA after 9/11,' *Theoretical Criminology* 2017,1362480616684195.
[15] Ibid.
[16] C. Murphy, *supra* note 10

especially in the human rights sensitive area of counter terrorism. These challenges include inter alia the difficulty of parliamentary and judicial oversight and the problem of securitization, which describes the progressive framing of more and more social problems as threats that need to be addressed by a secretive security policy.[17]

At EU level, the powers to adopt measures in the field of intelligence in the context of the fight against terrorism are exercised in either the area of freedom, security and justice (AFSJ) or in the common foreign and security policy (CFSP). What determines the use of one competence or the other, however, is not entirely clear. Yet, the distinction is of crucial importance because the two systems differ radically in terms of procedures, the powers of the involved institutions and the guarantees for individuals, including judicial oversight.[18] Parliamentary oversight and the review of Union acts remain significantly limited in the sphere of the CFSP (Art. 31 TEU, Art. 275 TFEU), leading to a dynamic in which security related aspects are over emphasised, while human rights and civil liberty implications of external actions are often neglected.[19] Nevertheless, the linking of internal and external capacities is one of the main objectives of EU counter-terrorism policy.[20] While it is evident that EU operational capacities to collect intelligence are still at a very limited stage compared to the capacities of nation states, the exchange of nationally processed information through EU institutions has seen significant integration. In order to conceptualise this exchange, it is beneficial to make an analogy to US American Fusion Centers: The characteristics of such entities, most importantly the arrangement of an array of people and organizations to be contributors as well as consumers of intelligence, the fusing of a broader range of data, including non-traditional source data, the interlink function between different layers of federal actors and an analysis driven proactive threat identification approach.[21]

1.2. IDENTIFICATION OF THE RESEARCH QUESTION

With the key concepts of EU counter terrorism intelligence exchange established, the following research question was identified:

(RQ): To what extent does the existing EU regulatory framework on the sharing of intelligence information for countering terrorism respect the rights of individuals?

[17] J. v. Buuren, 'Secret Truth. The Eu Joint Situation Centre.,' *Amsterdam: Eurowatch* 2009
[18] P. P. Craig and G. De Búrca, *Eu Law: Text, Cases, and Materials* (Oxford: Oxford University Press 2015).
[19] F. Trauner, 'The Internal-External Security Nexus: More Coherence under Lisbon?,' *EU ISS Occassional Paper* 2011 35
[20] Council of the European Union, *supra* note 4
[21] D. L. Carter and J. G. Carter, *supra* note 3

The question encompasses explanatory, hermeneutic, evaluative and exploring characteristics. In order to systematically address the core issues of the question, three sub questions were identified, the first one being:

(SQ1): What is the level of protection guaranteed by the EU to the rights to privacy and data protection?

This question will address the issue from the perspective of EU primary law by analysing the basic privacy rights that need to be respected in EU actions. Conducted in an evaluative, but also in an exploring way, the respective chapter will deliver a teleological interpretation of the generated knowledge in the light of the Union's moral principles. To identify the current regulatory framework in which non-military actors conduct intelligence sharing activities directed at countering terrorism, the second sub question was constructed as follows:

(SQ2): What is the current regulatory framework for EU non-military actors concerning counter terrorism intelligence cooperation?

The question is designed in an explanatory and hermeneutic way to obtain relevant knowledge concerning the legal bases of counter terrorism intelligence exchange and its actual implementation in the area of freedom, security and justice.

The issue of intelligence exchange is, however, not limited to actors operating in this framework, the following sub question therefore addresses the respective mandate and actions of military actors:

(SQ3): What is the current regulatory framework for EU military actors concerning counter terrorism intelligence cooperation?

This question analyses the counter terrorism intelligence sharing activities conducted by actors in the framework of the common foreign and security policy. Like SQ2, it encompasses explanatory and hermeneutic characteristics. Chapter three and four thus provide an argumentative evaluation of the constitutional mandates of identified actors in the field of EU counter terrorism intelligence sharing, found primarily in the Articles 67 (3), 87 (2a) and 88 (2a) TFEU and Articles 24 (1) and (3) TEU. The recent developments in the chosen policy field will be analysed by comparing the relevant Council decisions and EU policy documents with the hermeneutical interpretation of the treaty provisions. Since the EU has repeatedly engaged in the conclusion of agreements that included provisions on intelligence exchange, a last sub question will evaluate whether this external exchange is in exercised accordance with the Union's internal protection standards:

(SQ4) To what extent are the agreements concluded by the EU with third countries on the sharing of intelligence information compatible with its internal standard of protection?

The sub question encompasses hermeneutical, logical and evaluative elements. The fith chapter will subsequently address the specific issues raised by the conclusion of intelligence-exchange agreements with third countries. The accordance of such agreements with the EU's internal privacy protection standards will be evaluated via systematic approach, analysing the coherence and consistency of agreement provisions with EU data protection standards. A purposive interpretation will be applied to the treaty provisions on the conclusion of agreements in the fields of the AFSJ and the CFSP.

2. THE HUMAN RIGHTS DATA PROTECTION STANDARDS OF THE EU

This chapter will evaluate the level of protection guaranteed by the EU to the rights to privacy and data protection. It introduces the most relevant Treaty provisions, secondary legislation acts as well as case law; and subsequently discusses the general level of protection.

2.1. PROVISIONS OF THE LISBON TREATY

The Lisbon Treaty reaffirmed the founding values of the Union and brought important reforms regarding their protection, most significantly through giving the Charter of Fundamental Rights of the European Union the same legal effect as the Treaties (Art. 6 (1) TEU). In the following, an overview over the most important provisions in primary law will be given.

2.1.1 THE VALUES OF THE UNION ENSHRINED IN ARTICLE 2 TEU

Since the Treaty of Amsterdam in 1997, Union primary law explicitly stated that 'the Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law', principles which were later adapted and became the 'values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities' (Art. 2 TEU). The emphasis that the Union is 'founded' on these values rather than having to simply respect them underlines that they are defining a 'political morality' for the EU legal and political system as a whole, reflecting modern European constitutional tradition.[22] Member states can be sued for a 'serious breach' of these values (Art. 7 (1) TEU) and new members have to comply with them to be accepted into the Union (Art. 49 TEU). Of particular interest is the value of the rule of law, as it was established in *Les Verts* v. *Parliament* that in the light of this principle the measures of institutions and member states have to be adopted in conformity with the primary sources of Community law.[23] This doctrine points out that the interdependent, organic entity that the rule of law forms with the other values of Article 2 TEU[24] has indeed an important standing within the EU legal order, as it '*provides the foundation for judicial review and implies the existence of comprehensive and complementary judicial review processes'*, giving the judiciary the authority to test taken measures for their compliance with the principles of legality and judicial protection.[25] It could be

[22] L. Pech, ''A Union Founded on the Rule of Law': Meaning and Reality of the Rule of Law as a Constitutional Principle of Eu Law,' 6 *European Constitutional Law Review* 2010,359-396.
[23] ECJ, Case 294/83 *Les Verts* v. *Parliament* [1986]
[24] Pech states that given that the principle of the rule of law is almost always accompanied by the principles of liberty, democracy and respect for fundamental rights in the treaties, the EU legal order does not support a doctrinal interpretation of 'rule of law' as an independent principle. See L. Pech, *supra* note 22
[25] Ibid.

argued here that in regard to the issue of counter terrorism intelligence exchange, the values of Article 2 TEU are directly concerned: A community based on the rule of law would need to review all actions taken within its institutional framework in regard to its founding principles, hence in an exchange of nationally collected security data, compliance with the Union's values would need to be ensured in the process of sharing as well as in regard to the acquisition of the shared data. However, potentially due to the lack of closer definitions for principles like freedom, democracy or rule of law, there have been no substantial cases in which the ECJ used the respective values of the Union as a direct means of judicial evaluation, but rather tested EU measures in regard to more concrete principles, particularly specific fundamental rights. Furthermore, the '*virtuous circle*' that reinforces the community of law through the dynamic between the enforcement and review of legal acts has been problematic outside of the former first pillar.[26] Yet, this does not in turn imply that Article 2 TEU has no influence on the protection of human rights and personal data within the EU. Rather, the Union's founding values can be considered to be an underlying justification to review EU measures for their compliance in a framework of common political-moral standards.

2.1.2. ARTICLE 16 TFEU AND 39 TEU

The Treaty of Lisbon introduced Art. 16 TFEU as a stronger legal basis for data protection that grants individuals the '*right to the protection of personal data concerning them*' (Art. 16 (1) TFEU). It also provides that the Council and the Parliament need to determine data protection rules for all Union institutions as well as Member states when operate within EU law, including the regulation of data movement, and that these rules are to be controlled by independent authorities (Art. 16 (2) TFEU). A clear exception from the ordinary legislative procedure is the policy field of the CFSP, in which the same standards are applied while derogating from the rights of the European Parliament (Art. 39 TEU). This derogation from parliamentary oversight reaffirms the more intergovernmental structure that distinguishes the CFSP from other EU policy fields for the issue of data protection, a drawback that will be further assessed in the subsequent discussion on the necessity of distinguishing between police and military cooperation. The extensive scope of Article 16 is potentially limited by Declaration 20 on Article 16 of the Treaty on the Functioning of the European Union, as it establishes that special attention on the matter will be taken in regard to rules with '*direct implications for national security*'. The scope of the Articles' application is further reduced by Declaration 21 on the protection of personal data in

[26] C. Murphy, *Eu Counter-Terrorism Law - Pre-Emption and the Rule of Law* (Oxford: Hart Publishing 2012).

the fields of judicial cooperation in criminal matters and police cooperation, which reaffirms the '*special nature*' of the fields of judicial cooperation in crime matters and police cooperation, noting that special rules might need to be established in regard to data protection and data exchange. Furthermore, the extensive derogation rights granted to the United Kingdom, Ireland and Denmark in regard to police and judicial cooperation in criminal matters have led some to the conclusion that at least for these three states, the former pillar structure of Union law is still intact.[27] Despite such limitations, the inclusion of specific data protection provisions for the action of Union institutions into primary law can still be considered as an essential step ahead in the commitment to offer a wide range of data protection within the Union.

2.1.3. THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EU

The binding legal force that the European Charter of Fundamental Rights gained through Art. 6 (1) TEU has concrete implications for the exchange of intelligence within the Union. Of special relevance for the exchange of counter terrorism information are the rights to private and family life, home and communications, and the right to the protection of personal data (Art. 7, 8 CFREU). The establishment of an article solely dedicated to the protection of personal data can be regarded as a substantial improvement from previous conceptualisations of the freedom from disproportionate state communication supervision, especially in comparison with the European Convention of Human Rights. The less focused nature of Art. 8 ECHR did certainly not impede the European Court of Human Rights to scrutinise public authority in regard to state surveillance and to establish legal principles on the matter that had far reaching impact on the perception of data protection[28], neither did the CJEU sufficiently distinguish between the right to privacy and the right to data protection.[29] Nonetheless, it can be argued that Art. 8 CFREU has its own justification by offering a higher level of protection. First, it has been noted that the assessment of whether personal data is at stake or not is easier to assess than an infringement of privacy,

[27] See H. Hijmans, 'Recent Developments in Data Protection at European Union Level,' 11 *ERA Forum* 2010,219-231. Hijmans concerns could be regarded as validated by Denmark's recent withdrawal from Europol, however the concluded agreement between Denmark and Europol reaffirms the validity of Art. 16 TFEU and the CFREU (Art. 10 (3) Agreement on Operational and Strategic Cooperation between the Kingdom of Denmark and Europol)

[28] Consider for instance ECtHR *Klass v. Germany*, Appl. No. 5029/71, 6 September 1978, in which the not only ECtHR established the principle that state surveillance capacity needs to be balanced with individual rights, but also ruled that individuals do not need to prove their specific victim status within surveillance programs of great scale and secrecy to gain access to judiciary.

[29] See O. Lynskey, 'Deconstructing Data Protection: The 'Added-Value of a Right to Data Protection in the Eu Legal Order' ' 63 *International and Comparative Law Quarterly* 2014,569-597., for a detailed analysis of how the CJEU repeatedly missed the opportunity to consistently distinguish between the two respective rights both prior as well as post the entry into force of the Lisbon Treaty, leading to the impression that data protection might be a mere subset of the right to privacy.

which in comparison is highly context dependent.[30] As the right to data protection covers '*any operation or set of operations which is performed upon personal data, whether or not by automatic means*'[31], it covers all aspects related to the automatic storing of data and therefore also encompasses cases in which publicly available or otherwise non-privacy intrusive data are involved, offering a broader range of protection. This protection can enhance individuals' informational self-determination through enabling a '*selective presentation*' of different personal traits in different social and digital environments, reducing a danger for misinterpretation[32] that will be further discussed in section 2.4. Furthermore, the right to data protection can potentially reduce informational power asymmetries between data subject and data processor and therefore more adequately balance a relationship that might otherwise be significantly tilted in the direction of the processor.[33]

When reviewing intelligence exchanges measures on an EU level, it is additionally necessary to take the non-discrimination dimension of fundamental rights into account that finds its expression in Art. 21 (1) CFREU and has an additional legal basis in Art. 18 TFEU. This right is of special relevance because it has been noted that citizens from different member states are subjected to disproportionate levels of surveillance based on their nationality, and further that the sharing of such 'tainted' information is a key challenge to effective human rights protection on the EU intelligence cooperation level.[34] As the non-discrimination provisions in primary law specifically state that within the scope and application of the treaties, no such discrimination should occur, the tension added to the issue by the right to non-discrimination stems from the reduced likelihood that national intelligence services have the same civil rights review mechanisms in check when monitoring individuals abroad as they have for the collection of intelligence from citizens of their respective countries, yet the acquired data would need to comply with the EU human rights protection standards when it is shared through Union institutions. While this problem is in principle applicable since the CFREU gained full legal force, its implications became unprecedently clear in the context of the Snowden Affair of 2013. The revelations showed large scale electronic surveillance of foreign communications conducted by several EU Member States intelligence agencies, which quickly raised the question as to whether those agencies had shared information on EU citizens without the knowledge of their home

[30] Ibid.
[31] *OJ* [1995] L 281/31, 23.11.95, Art. 2 b
[32] Lynskey, *surpa* note 29
[33] Lynskey, *supra* note 29 elaborates on the difficulty for individuals to assess the potential harmfulness of their collected data, which reduces the likelihood of an informed decision, the problem of accountability that stems from not being able to identify the responsible processing actors and the reduced bargaining power of the data subject.
[34] Cf. section 3.2 in Bigo et al., *supra* note 6

country to the NSA and its allies, effectively breaching the solidarity principle.[35] Within the EU, it is less likely that intelligence that was intercepted in such a way is shared with the other Member States, as this would give the recipients insight into the surveillance capacities of the sharing party. It is, however, on the other hand imaginable that there might still be incentives for such exchanges, especially if it would offer Member States the possibility to gain intelligence that their own agencies could not have conducted under their respective safeguards concerning internal communication.

It can therefore be stated that when reviewing counter terrorism intelligence exchanging acts of the EU, the Art. 7, 8, and 18 of the CFREU are the most relevant standards of human rights protection within the EU. The Charter is, however, not universal in nature: Art. 51 (1) CFREU provides that it only applies to Union bodies and institutions, and to the Member States only insofar as they implement Union law. Additionally, it cannot establish new powers and tasks of the Union or modify existing ones (Art. 51 (2) CFREU).

2.2. SECONDARY DATA PROTECTION LEGISLATION

In order to specify and govern the scope and application of the fundamental rights and values outlined in 2.1., the EU institutions drafted legislation covering data protection standards, however general provisions on the exchange of data in criminal procedures remain rather scarce and target specific solutions are more commonly applied.

The Directive 95/46/EC 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 can be regarded as the main piece of legislation covering the processing and protection of personal data. It serves a dual purpose, scilicet the protection of fundamental rights and freedoms of natural persons, in particular their right to privacy[36], on the one hand, and the ensuring of the free flow of data between Member States[37], on the other. It contains important safeguards, including obligations to fair and lawful processing, accuracy and purpose and time specific storing[38], and lays out criteria for legitimate processing.[39] However, the directive was excluded from covering aspects outside of the former first pillar, and therefore explicitly did not apply to ‘processing operations

[35] Ibid. Bigo et al. mention the intelligence agencies of the UK, Sweden, France, Germany and the Netherlands as examples for large scale surveillance of foreign communications.
[36] Directive 95/46 EC of the European Parliament and 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, OJ [1995] L281/38 24.10.1995, Art. 1 (1)
[37] Ibid., Art. 1 (2)
[38] Ibid., p.40, Art 6 (1)
[39]Ibid., Art. 7.

concerning public security, defence , State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law'.[40]

This led to a mosaic of data protection legislation within the AFSJ that is targeted to specific institutions, for example Europol, with the only general data protection document dedicated to criminal procedures currently in force being the Council framework decision of 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[41] Similar to the general data processing and movement directive, the framework decision has a dual objective in which two aims are sought to be balanced, in this case the fundamental rights and freedoms of natural persons on the one hand, and a high level of public safety, on the other.[42] The framework decision further has a notion of balancing the tense relationship between national action and hence sovereignty in security matters with the need to comply with Union fundamental rights on the Union level: The council cautiously rules out any inference stemming from the decision on future competences of the Union to regulate the national collection and processing of personal data[43], yet acknowledges the need to apply common rules 'concerning the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed lawfully and in accordance with fundamental principles relating to data quality'.[44] Indeed, the provisions of the framework decision lay down some common standards, including obligations for the processors, hence the member states, and rights for the data subjects whose data is processed and shared. Among the most important processor-obligations are the principles of lawfulness, proportionality and purpose, the erasure of data, the establishment of time limits for data storing and the provisions on the exchange with competent international authorities and third states. The council essentially mirrors the arguments for a strong right to data protection by issuing safeguards which treat the collection and exchange of data *as such* as an intrusive measure that needs to be carefully regulated. This preference over a type of legislation that determines the intrusiveness of specific collection and exchange procedures in regard to their implications for the right to privacy subsequently reaffirms the legitimacy of the right to data protection as a fundamental right independent from the right to privacy. The dangers of automatic processing that have served as a justification for this independent stance have also found acknowledgement in the establishment of safeguards

[40] Ibid., p.39, Art. 3 (2)
[41] *OJ* [2008] L 350/60, 30.12.2008
[42] Ibid., p.64, Art. 1 (1)
[43] Ibid., p.61, Recital 7
[44] Ibid., Recital 11

concerning the automated processing of individual data[45] and the limitation of the exchange of 'special categories of data', including for example racial origin or union membership.[46] Adding to these obligations, individual fundamental rights have been considered, most importantly the rights of information and access, which strengthen transparency, the right to rectification, erasure or blocking and the right to compensation.

While the overall content of the framework decision reaffirms important Union data protection standards, its implementation is highly dependent on the member states and while there is a provision to set up national supervisory authorities to monitor compliance of the decision with national procedures, no EU authority was established as an independent observer. Furthermore, the decision is 'without prejudice to essential national security interests and specific intelligence activities in the field of national security'[47] which gives member states a high possibility for derogation, especially in the realm of counter-terrorism. Its scope is also rather limited, as it does apply neither to the institutions of Eurojust and Europol nor to information exchange systems such as the Schengen Information System (SIS).[48] However, being the only general document that is currently governing information exchange in the area of the AFSJ, it can still be regarded as a vital component of the EU human rights and data protection regime and a reconfirmation of its respective principles. In the future, the current Data Protection Regime will be replaced by the Regulation 2016/679 and Directive 2016/680, which will offer a more extensive and comprehensive level of protection.[49]

2.3. CASE LAW

In the following, the most relevant cases judged by the CJEU in regard to privacy and data protection and the access of public institutions to personal data will be introduced. Prior to the Lisbon Treaty, the AFSJ was only subject to the jurisdiction of the Court to the extent Member States voluntarily allowed it and the CFSP is still largely excluded from the courts judgement in the current EU legal order (Art. 17 (1), 24 (1) TEU) Therefore, case law that holds implications for this study is highly limited.

[45] Ibid., p.66, Art. 7
[46] Ibid., Art. 6
[47] Ibid., p.64, Art. 1 (4)
[48] Ibid., p.63, Recital 39
[49] Cf. Section 2.4

2.3.1. THE PASSENGER NAME RECORD CASES

After the United States of America framed Passenger Name Records (PNR), which are digital records of the itinerary of an airline passenger or a group of passengers, as necessary instruments to combat terrorism after the devastating attacks of the 11th of September 2001, the USA concluded an agreement with the European Union on the exchange of such records in May 2004. The agreement was soon challenged by the European Parliament, which argued for annulment based on pleas of breach of the fundamental principles of the Directive 95/46/EC that the agreement was based on, breach of fundamental rights and breach of the principle of proportionality.[50] On the contrary side, the Commission and the United Kingdom argued that only private parties, rather than institutions of Member States, were involved and that the measure was therefore within the scope of Union Law.[51] In Case C-318/04, the Court reviewed the legality of the concluded agreement in regard to the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection. Directive 95/46/EC was identified as an incorrect legal basis, as the Court held that the transfer was conducted within a framework related to public security on the behalf of public authorities[52] and measures that were aimed at national security were explicitly excluded from the respective Directive. The Court argued in a similar way that the agreement could not be based on Article 95 EC, which was also considered to be an incorrect legal basis as its scope did not cover the public security measures that were at the heart of the cooperation.[53] The agreement was therefore annulled without a review of the extensive pleas related to the infringement of fundamental rights that were brought up by the parliament.

The judgement therefore clarified that information exchange for security matters needs a legal base that clearly relates to criminal investigation. This emphasised that developments in the internal and the external dimension of the AFSJ mutually reinforce each other, but also the difficulty in safeguarding and balancing the respect for fundamental rights in international agreements.[54] However, the judgement was also seen as a missed opportunity to examine the concerns raised by the parliament regarding the proportionality and fundamental rights implications of PNR transfers.[55]

---

[50] ECJ, Case C-317/*04 European Parliament* v *Council* and Case C-317/04 *European Parliament* v *Commission*, [2004], para.50
[51] Ibid., para.53
[52] Ibid. para.58
[53] Ibid., para. 68
[54] B. Van Vooren and R. A. Wessel, *Eu External Relations Law : Text, Cases and Materials* (Cambridge, United Kingdom: Cambridge University Press 2014).
[55] European Law Blog: 'Judgment in PNR cases: Cases C-317/04 and C-318/04', available at: http://eulaw.typepad.com/eulawblog/2006/05/judgment_in_pnr.html

2.3.2. C-524/06, HUBER V. GERMANY

The Court was appealed to review the application of Art. 12 (1), 17 and 18 of Directive 95/46/EC in December 2008 in a case that involved Austrian national Heinz Huber requesting his personal data to be deleted from a file held by the German Office for Migration and Refugees. The database, which was supposed to be used primarily for statistical purposes and was only made available to criminal justice authorities to if it would need be used in the investigation of criminal matters or threats to public security[56]. Huber regarded this as an act of discrimination because no such system was in use for German nationals.[57] The Court ruled that while the collection of information by Member States on foreign nationals could be necessary to monitor population movement and the objective of fighting crime through the database was legitimate, the storage of personal information of only non-nationals was a discrimination that was illegitimate under the law of the European Community Treaty.[58]

The judgement can be interpreted to have several implications. On the one hand, it affirmed data processing aimed at managing immigration, including law enforcement, as a legitimate use of power. On the other hand, it reaffirmed the purpose specification principle by posing strict limits to the scope of processed data, which should not exceed the amount of data that was necessary to fulfil the original task it was collected for. Most importantly, however, the judgement can be interpreted as an enforcement of the non-discrimination rule in criminal matters: Data processing and storage for law-enforcement purposes are only lawful if they affect all Union citizens equally, regardless whether they are citizens of the state who processes the data or not.

2.3.3. JOINED CASES C-293/12 AND C-594/12

In 2014, the non-governmental organisation Digital Rights Ireland challenged the EU Data Retention Directive of 2006, a case that was subsequently referred to the ECJ. The organisation held that the Directive, which obliged all telecommunication service providers operating in Europe to retain a wide variety of metadata from their subscribers for a period of six months to two years, was incompatible with fundamental rights. After stating that an interference with the right to privacy was possible regardless of the level of inconvinience caused to the data subjects, that the right to data protection was at stake simply because processing of personal data was governed and that a review of the Directive with the Articles 7 and 8 CRFEU was therefore

[56] ECJ, C-524/06, *Huber* v. *Germany* [2008], p.42
[57] Ibid., para. 32
[58] Ibid., para. 58, 49 and 80

necessary,[59] the Court applied a proportionality test to the Directive. It found that while the retention of the data and the access of the authorities on it was suitable to achieve its purpose as a tool of criminal investigation[60], it did not lay down clear and precise rules regarding the extent of the interference with individual rights[61] and the Directive was therefore annulled. The Court laid down several requirements that legislation interfering with individual privacy and data protection rights would need to fulfil, including substantive and procedural conditions and sufficient protection of the retained data in the respective storing systems.[62]

The judgement provided a landmark case for the issue of privacy in the digital age, as the court applied for the first time a proportionality test to public action aimed at security. It was interpreted to acknowledge the dominating power that can stem from access to bulk metadata of entire populations[63] and the ruling was therefore considered to be a rectification approach to what was considered an arbitrary use of power by the judges.[64] On the other hand, it did not render data retention as such as unconstitutional and incompatible with the right to privacy.[65]

2.3.4. JOINED CASES C-203/15 AND C-698/15

The CJEU had to decide on two further data retention cases in December 2016. Having invalidated the general EU data retention regime in 2014, the court was now asked to deliver a preliminary ruling regarding the interpretation of Article 15(1) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector in the light of Articles 7 and 8 CFREU.[66] The review was necessary for rulings on the national data retention laws of Sweden and the United Kingdom that were pending in their respective national courts.

The Court repeated the arguments brought forward in its Digital Rights Ireland Judgement, including the threat of a limitation of freedom of speech through an impression of constant

[59] ECJ, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014], para. 33 and 36

[60]Ibid., para.49

[61] Ibid., para. 65

[62] The court identified criteria for limiting the number of persons who have access to the data as an example for conditional, review mechanisms consulted prior to the accessing as procedural conditions. Ibid., p.60-62

[63] A. Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd V Minister for Communications,' 78 *The Modern Law Review* 2015,535-548.

[64] Ibid.

[65] Ibid.

[66] ECJ, Joined Cases (C-203/15) and (C-698/15), *Tele2 Sverige AB* v *Post- och telestyrelsen***,** and *Secretary of State for the Home Department* v *Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales* [2016], para. 1

surveillance.[67] The principle that factual grounds of suspicion were necessary for the retention of data was upheld, but also amended by the possibility to retain data from a certain geographical area.[68] For national laws to be compliant with EU law, it was held that they would need to ensure clear rules concerning the scope and application of the data retention and the establishment of minimum safeguards.[69] Important to note regarding the right to data protection is that the court seemed to see the retention of data as a precondition for processing and therefore interpreted it under the privacy safeguards that apply to the latter.[70] While the judgement was acknowledged as a confirmation that blanket retention of data is incompatible with the CFREU regardless if conducted at EU or national level,[71] it was also criticised for its uncritical stance on geographic and group profiling.[72]

2.4. FUTURE SECONDARY LEGISLATION

As mentioned in 2.3., the EU human rights and data protection framework has been renewed and extended by Regulation 2016/679 and Directive 2016/680. In the following, Directive 2016/680 will be shortly reviewed in regard to its implications for future counter terrorism intelligence exchange.

Rather than defining rules for the exchange of data among Member States, the Directive establishes for the first time common processing rules for competent authorities of the Member States 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*'.[73] This means that the legality of data transfers is no longer ensured through the compliance of the transfer with the Union's fundamental rights, but through the compliance of the data itself. The Directive reaffirms the rights of the individual as outlined in 2.2., as well as the principles relating

[67] Ibid., para. 100 and 101
[68] Ibid., para. 105 and 106
[69] Ibid., para 109
[70] G. Beck, 'Case Comment: C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom Watson & Others', *Eutopia Law* 2017, available at: https://eutopialaw.com/2017/01/13/case-comment-cases-c-20315-tele2-sverige-ab-v-post-och-telestyrelsen-and-c-69815-secretary-of-state-for-the-home-department-v-tom-watson-and-others/
[71] O. Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change', *European Law Blog* 2017, available at: https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/
[72] Ibid.
[73]Directive 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 *OJ* [2016] L 119/105, 4.5.2016, Art. 1 (1)

to the processing of personal data.[74] At the same time, some adjustments necessary for the specific circumstances of law enforcement have been made, mainly in the rights of information and access. As a basic necessity for efficient criminal investigations, these rights were limited for individuals that are subject to such investigations, but also on the ground of protecting public or national security.[75] Member States however have to specify the processing operations they frame as the latter and also have to provide factual or legal reasons on their decision to deny access on such grounds.[76] An important innovation is further the distinction between different types of data subjects, including suspects, convicts, victims and other parties to a criminal offence, whose data is to be processed in a clearly distinguished manner.[77] Transfers of data into third countries are dependent on the level of protection in the receiving country, which includes the rule of law, respect for fundamental rights and the existence of independent supervisory authorities.[78] Data protection is further strengthened through the principle of data protection by design and by default, while transparency is enhanced through the requirement of logging the processing operations and keeping a respective record.[79] Data Protection Officers who inter alia monitor the compliance with the Directive need to be appointed.[80] Regarding the consistency of the directive's application, independent supervisory authorities are to be appointed by the Member States who shall have investigative powers to monitor compliance with the Directive and the lawfulness of processing activities.[81]

While some important limitations remain, the Directive, which will apply to Member States from the 6th of May 2018,[82] can be expected to have a profound impact on counter terrorism intelligence exchange. It establishes a regulatory framework that provides extensive safeguards for individuals whose data is processed by national law enforcement institutions and further requires essential review mechanisms. Although the ultimate protection of these common standards will be dependent on their transfer into national law, a basic level of protection can be assumed. This might substantially reduce the danger of unlawfully conducted information to enter intelligence exchange systems on the Union level and therefore has the potential to ensure those systems' compliance with Union fundamental rights. The framework further codifies several concerns of the CJEU by reaffirming the standards the court set out for the adequacy of

[74] Ibid., p. 107-113, Art. 4-18
[75] Ibid.,p 110-11, Art. 13 (3), 15 (1)
[76] Ibid., Art. 13 (4), 15 (2, 5)
[77] Ibid., p.108, Art 6
[78] Ibid., p.120, Art. 36 (2)
[79] Ibid., p.113-116, Art. 20, 24, 25
[80] Ibid., p.119, Art. 33, 34
[81] Ibid., p. 123-128, Art. 41-51
[82] Ibid., p 130, Art. 59

transfers to third countries[83] and the purpose specification principle. Collection for specified, explicit and legitimate purposes principally does not allow for bulk data collection and might therefore establish a new regulatory safeguard for Art. 8 CFREU that is consistent with the court's rulings on data retention. Finally, the common standards also reduce the danger of discrimination, as they apply to all individuals regardless of their nationality.[84] However, it should be noted that the Directive does not apply outside the scope of Union law. In conjunction with Recital 14, this specifically includes

activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU).[85]

This does not only create a contradiction with Art. 1,[86] but also excludes secret services and other intelligence actors operating in the securitised arena of national security from the scope of the Directive. Therefore, the risk of fundamental rights breaching intelligence being exchanged within the Union is not reduced for all exchanging parties equally.

2.5. CONCLUSION AND CONTEXTUALISATION

The level of protection offered by the EU regarding human rights and data protection can be characterised as a manifold issue when regarding the regulatory frameworks' impact on the exchange of counter terrorism information within the Union. Although counter terrorism cooperation is a field of integration in which national security interests are at stake and intergovernmentalism therefore traditionally had and has a strong stand, the EU has not failed to take the rights of individuals into account when governing the exchange of intelligence, which might not least be related to the Union's long-standing commitment to its values and the rule of law. Especially the entry into force of the Treaty of Lisbon has brought substantial progress, mainly due to the binding legal force given to the CFREU and the abolishing of the former pillar structure that led to the inclusion of the AFSJ into the ordinary legislative procedure and the

[83] C.D.F. Maesa, '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)', *Eurojus.it* 2016, available at: 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/
[84] *OJ* [2016] L 119/105, 4.5.2016, Recital 17
[85] Ibid., p.91, 4.5.2016, Recital 14.
[86] C.D.F. Maesa, *supra* note 83

jurisdiction of the CJEU. The Charters' Articles 7, 8 and 21 offer a considerable level of protection to individuals' right to privacy, data protection and non-discrimination, which can in turn be expected to have a profound impact on the EU intelligence exchange regime. While the right to privacy used to be most commonly referred to by the CJEU,[87] the right to the protection of personal data is expected here to have an even higher impact on counter terrorism intelligence legislation and actions. It can be argued that through rendering the acquisition and therefore also the exchange of personal data by state authorities as an intrusive act itself, rather than requiring a proof for the level of intrusion exerted on an individual, the right to data protection is more adequately equipped to address the challenges raised by 21st century data processing. For instance, data protection can safeguard the individual from disproportionate treatment or even discrimination by requiring that human attention is given to an individual case, which could significantly reduce the danger of unjust treatment resulting from automatic processing or a shift of data from one source to another.[88] In the realm of counter terrorism action, such safeguards are all the more important, since an investigation against an individual can be expected to have deep impacts on the suspect's life and freedom. However, not only the prosecution itself, but also the fear of prosecution needs to be considered. A pre-emptive approach to counter terrorism that involves massive data retention of unsuspected individuals can exert a considerable level of conformity pressure, effectively limiting, if not controlling, the individual's behaviour.[89] This harmful potential was also recognised by the CJEU when it delivered its judgement in the cases of C-293/12 AND C-594/12, where it followed the Advocate General in stating that

'*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*'.[90]

Therefore, Art. 7, 8 CFREU and the recognition of the right to data protection in TEU (Art. 39) and TFEU (Art. 16) pose an imperative for the processing of personal data by state authorities and offer a profound level of protection that should be respected also in data exchanges on the Union level. An additional important point for such exchanges is the right to non-discrimination, as a situation in which Member States would be able to collect more data from other Member States nationals than they would be allowed to gather from their own citizens, and subsequently exchange this data with the foreign nationals' home country, would sufficiently undermine the

[87] See Lynskey, *supra* note 29, Section II B
[88] Ibid.
[89] Murphy, *supra* note 26
[90] ECJ, C-293/12 and C-594/12, p.37

content and scope of individual fundamental rights. Case C-524/06 *Huber* v. *Germany* provides an important example by ruling that Member States are precluded from applying systems for the purpose of fighting crime that process only the data of non-national Union citizens, but does not answer all questions related to the matter. While it can be assumed that such ruling could also apply to systems that disproportionately monitor foreign nationals in other Member States, which would have a deep impact on the actions of national intelligence services, the level of protection for Non-Union citizens is left ambiguous. It can be assumed that their data is more likely to be processed for reasons held as legitimate by the Court, such as statistical purposes and the evaluation of their right of residence. The conditions under which such data can be accessed by counter terrorism authorities are in principle covered by Art. 3 of the 2008 Council Framework Decision, but are in the end determined by the Member States.

While this leads to the conclusion that in principle, the EU human rights and data protection regime offers some important safeguards even in the sensitive matter of counter terrorism, it has to be noted how closely the actual protection is linked to the issue of transparency. The rights given to individuals can only be defended by the judiciary if there is sufficient clarity among the public about what actions are taken and what data is processed and exchanged.[91] Given the secrecy of national security matters and the fact that even in areas where uniform rules principally apply, Member States are not controlled in regard to their implementation, this might be one of the most essential problems in the protection of individuals' fundamental rights in counter terrorism intelligence exchange.

In a final remark, a fundamental distinction concerning the protection level as outlined above needs to be made between the AFSJ and the CFSP. While the AFSJ features a multitude of target specific data protection frameworks given to individual actors which will be analysed in the following chapter, it can nevertheless be stated that since it is covered by the jurisdiction of the CJEU and is subject to parliamentary oversight, the EU individual rights protection regime is present and enforceable within the AFSJ.[92] In comparison, the CFSP lacks not only any general framework concerning the protection and exchange of data other than the constitutional principles of the treaties, but also the possibility for judicial review. In absence of data protection guidelines in military matters, the Commission seems interestingly to favour the application

[91] See, for instance, the analysis of the Electronic Frontier Foundation concerning the strategy pursued by Digital Rights Ireland, retrievable at: https://www.eff.org/node/81899

[92] Noteworthy limits to the enforceability of AFSJ procedures arise from Art. 4 (2), 73 and 276 TFEU, as discussed below in 3.1.

Directive 95/46/EC despite its clear preclusion from national security matters,[93] however the question on the framework for military actors will be more adequately explored in Chapter Four.

Having explored the basic level of protection regarding privacy and data protection guaranteed by the EU in this Chapter, the question arises to what extent these safeguards are reflected in the regulatory frameworks of relevant EU actors who are tasked with fighting terrorism. The following chapter will do so by analysing the relevant legislation that applies to non-military actors.

[93] An indication for this can be found in the Commission Communication, *supra* note 5, as the Commission indicates the Directive as the correct protection document for its proposed Hybrid Threat Fusion Cell, which would be an intelligence processor with highly militaristic function.

3. THE REGULATORY FRAMEWORK FOR NON-MILITARY ACTORS

A vital component of the exchange of counter terrorism intelligence within the EU is conducted by non-military law enforcement authorities. This chapter reviews the regulatory framework for such exchanges among Union bodies and Member States, starting with a review of both primary and secondary legislation. It then goes on with discussing this framework in the light of the information that is available on the implementation and execution of counter terrorism intelligence exchanges among non-military actors.

3.1. PRIMARY LAW PROVISIONS

The primary Treaty provisions concerning the intelligence cooperation of non-military actors can be found in Art. 87 and 88 TFEU. Article 87 (1) lays down guidelines for the establishment of

'police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences.'

The mandate for regulating the processing of information can be found in 87 (2 a, c), which enable the collection, storage, processing, analysis and exchange of information and the possibility to establish common investigative techniques. Legislative acts are to be concluded by the ordinary legislative procedure.

Art. 88 TFEU provides more specific rules on Europol, stating that its mission shall be

'to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy'.

It is noteworthy that in conjunction with Art.88 (2a), which defines the '*collection, storage, processing, analysis and exchange of information, in particular that forwarded by the authorities of the Member States or third countries or bodies*' as a specified task of Europol, the TFEU tasks Europol with an express competence for counter terrorism intelligence exchange.

The scope of competences given to the EU by the TFEU as outlined above needs to be seen, however, in the light of Art. 72 and 73 TFEU, which state that Title V should neither affect the Member States' exercise of maintaining law and order and national security nor their capacity to organise between themselves the cooperation of their administrations in national security matters. In conjunction with Art. 4 (2) TEU, which provides that '*national security remains the sole*

responsibility of each Member State', a '*rule regarding the division of powers between the EU and the Member States as regards the execution of operational measures necessary to implement EU rules'* is therefore established.[94] Furthermore, Art. 276 TFEU holds that

'*the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security*',

which leads to the conclusion that the CJEU holds no jurisdiction to review the operational acquisition of intelligence by national agencies. However, this does not rule out the application of the CFREU provisions to national legislation that governs intelligence gathering, which was recently highlighted in the *Tele Sverige* judgement referred to in section 2.3.4. EU norms adopted under Art. 87 (2) TFEU, such as Directive 2016/680, can also be reviewed by the court and therefore continuously open the criminal justice sphere of the Member States to the investigation of the court.

3.2. EUROPOL

The European Union Agency for Law Enforcement Cooperation, while having little operative capacity, functions as a central node for the exchange of information for national law enforcement agencies.[95] Europol's fields of action were complemented to include the fight against terrorism by a December 2002 Council Decision, which required Member States to create specialised national task forces with access to all relevant information in terrorism related investigations, and to share at least data which identify the person, group or entity; acts under investigation and their specific circumstances; links with other relevant cases of terrorist offences; the use of communications technologies and the threat posed by the possession of weapons of mass destruction.[96] Established as an EU agency in 2010[97], Europol's legal base has

[94] S. Peers, *Eu Justice and Home Affairs Law* (Oxford: Oxford University Press 2011).
[95] B. Müller-Wille, 'The Effect of International Terrorism on Eu Intelligence Co-Operation,' 46 *JCMS: Journal of Common Market Studies* 2008,49-73. Müller-Wille argues that Europol should primarily be understood as a platform for easier exchange of information, providing facilities and infrastructure.
[96] Council Decision of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP *OJ* [2003] L 16/68, 22.1.2003
[97] Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ* [2009] L 121/37, 15.5.2009

been updated in 2016,[98] which unified its regulatory framework with its data protection provisions. In the following, the respective documents will be briefly introduced, followed by an overview of its data processing actions.

3.2.1. NORMATIVE FRAMEWORK AND DATA PROTECTION PROVISIONS

Europol's legal basis was revised on the 11th of May 2016, for the first time with the inclusion of the parliament in the decision procedure. Regulation 2016/794, which entered into force the 1st of May 2017, reaffirms the special attention given to the matter of terrorism in EU criminal investigation procedures, being identified as '*one of the most significant threats to the security of the Union*'[99] and specifically referred to in five recitals, including the commitment to information exchanges with the private sector and third countries.[100] Preventing and combatting terrorism is a primary objective of Europol and the exchange of information as well as the support for Member State cross border information exchange activities are listed among its specific tasks[101], mirroring the express competence given in this regard by the TFEU. In the regulation, the operative arrangement of this mandate is interwoven with data protection provisions. Personal Data is allowed to be processed by Europol if the respective individual has been involved in a criminal offence, but also when it is suspected on '*factual indications or reasonable grounds*' to commit such offences in the future[102], therefore allowing for a pre-emptive approach. Furthermore, personal data may be processed if it facilitates the information exchange between Member States, other Union bodies, third countries and international organisations.[103] Data is made available through the mandatory Europol National Units, who act as liaison bodies within their respective Member State and are tasked with coordinating and enhancing the communication of all competent authorities with Europol.[104] They are assisted by Liaison Officers who hold a national office at Europol, facilitate multilateral intelligence exchange and can additionally organise bilateral cooperation outside Europol's scope, according to their national laws.[105]

[98] Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ* [2016] L 135/53, 24.5.2016
[99] Ibid., p.54, Recital 6
[100] Ibid., p.57, Recitals 30, 32
[101] Ibid., p.64-65, Art. 3 (1, 2 a, f)
[102] Ibid., p.74, Art. 18 (2, a)
[103] Ibid., Art. 18 (2, d)
[104] Ibid., p.66-7, Art 7
[105] Ibid., p.68, Art.8

Purpose and restrictions of the shared data, including access, transfer, erasure or destruction, are to be determined by the sharing party or by Europol if no such specifications were made, and further processing different from the original purpose is only allowed if the original provider allows to do so.[106] Access or use may also be restricted by Europol for information retrieved from publicly available sources.[107]

The ordinary procedure for the retrieval of information that was shared with Europol's systems works under a 'hit/no hit' system which alerts Europol that a request for data has been made, leading to the subsequent sharing of the data if the original provider gives its consent.[108] There is also a duty to notify Member States about information concerning them, which is however also conditional on the consent of the provider as long as no imminent threat for life is present.[109]
Europol is also allowed to exchange personal data with third countries or international organisations. Such transfers require, without prejudice to agreements concluded by Europol under its previous legal basis, an approval of the data protection offered by the third party concerned, which can be achieved by an adequacy decision issued by the Commission or sufficient data protection provisions in a concluded international agreement.[110] In individual cases, the Executive Director can also arrange the transfer of data without such safeguards and the Management Board can authorise sets of transfers for a renewable period of one year.[111] Additionally, exchanges can also be made with private parties under a variety of conditions, and information can be acquired from private persons.[112]

The new legal basis of Europol also includes Europol's general provisions on data protection, therefore unifying and updating the former Decisions 2009/371/JHA and 2009/936/JHA. It encompasses a wide variety of protection provisions that are congruent with Council Decision 2016/680, but also safeguards that are more specifically targeted at Europol's field of action. All data protection standards and individual rights referred to in 2.4. find their expression in Europol's respective provisions, in most cases offering an even more detailed level of protection.[113] Noteworthy is also the establishment of the '*data protection by design*' principle, which was not existent in Europol's previous legal basis and requires the institution to implement its technical and organisational measures and procedures with special regard to the rights of data

[106] Ibid., p.74, Art. 19
[107] Ibid.
[108] Ibid. Art. 18
[109] Ibid., p.76, Art. 22
[110] Ibid., p.78, Art. 25 (1)
[111] Ibid., p.76, Art. 25 (5, 6)
[112] Ibid., p.79-81
[113] For instance, the conditions for the use of and access to special categories data is strictly regulated, and specific time limits are established for the storage of data. *OJ* L 135/83, Art. 30, 31

subjects.[114] This approach of making privacy an integral part of the operative structure, '*a default mode intrinsically connected with it*', can be expected to produce more privacy sensitive measures than an ex-post application of privacy principles to an already existing measure or institution.[115]

Concerning transparency, the central instrument for the individual is the right of access for the data subject, granted by Article 36 of the Regulation, that holds that any data subject has '*the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol*'.[116] The information that is to be given shall contain information on if data is stored or not, nature of the data and available information on its source, indications for the legal basis of the processing and the storing period.[117] However, Europol can decide to restrict access to the data in a variety of cases and the access is further dependent on the consent of the providing Member State, which can object by a statement that such access would jeopardise ongoing investigations or '*be contrary to the essential interests of the security of the Member State concerned'*.[118]

The monitoring of the level of data protection in exchanges conducted through Europol is conducted both at EU and Member State level. Art. 41 requires the appointment of an independent Data Protection Officer, who has the task to observe the internal implementation of the Regulation, to promote the right of access and to document the use of personal data. However, the officer is only mandated with monitoring the processing of the data by Europol, not the legality of the data itself. Same applies to the mandatory national supervisory authorities, which are set up to observe whether transfers, retrievals or communication of personal data violate national law or individual rights and which are set up as contact points for individuals who want to exercise their right of access.[119] Additionally, the new Regulation provided for the supervision of the European Data Protection Supervisor, who now has similar monitoring rights as the internal Data Protection Officer, with an additional executive right to order the rectification, restriction, erasure or destruction of personal data and impose temporary bans on processing operations of Europol if they are in breach of the processing provisions. Parliamentary oversight was further enhanced by the establishment of a Joint Parliamentary Scrutiny Group (JPSG) that involves national parliaments as well as the European Parliament and that has a variety of access

[114] *OJ* L 135/85, Art. 33
[115] G. Valkenburg, 'Privacy Versus Security: Problems and Possibilities for the Trade-Off Model,' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds), *Reforming European Data Protection Law*(Springer Netherlands, 2015).
[116] *OJ* L 135/86, Art. 36 (1)
[117] Ibid., p.86-7 Art. 36 (2)
[118] Ibid., p.66, Art. 6 (2)
[119] Ibid., p.91-2, Art. 42

and review rights, including a yearly discussion with the EDPS on the protection of fundamental rights and personal data in Europol's actions.[120]

3.2.3. COUNTER TERRORISM DATA EXCHANGE ACTIONS

Europol's central base for storing information is the Europol Information System (EIS). As described above, it works under a hit/no hit system in which the output is determined by the restriction specifications of the providing Member State, who can then decide to contact the inquiring party. The database is fed by the national units, which might also involve automatic uploads by 'data loaders', programmes which have been installed in numerous national databases.[121] Intelligence is further stored in Analysis Work Files, an information processing system on specific crime areas that acts as a tool to '*simultaneously store, process and analyse factual information ("hard" data) and in particular "intelligence" (or "soft" data), including personal data of a sensitive nature*'.[122] The files contain much more sorts of personal data than the EIS and may also include the data of witnesses or victims.[123] Within these files, Analysis Projects (AP), formerly called focal points, are established. They focus on phenomena from a commodity based, thematic or regional angle.[124] The relevant analysis projects for counter terrorism intelligence exchange are the AP Hydra, dealing with islamist terrorism, the AP Travellers, dealing with returning foreign fighters, and the AP Weapons and Explosives.[125] Target Groups can be established as operational projects that can take the form of criminal intelligence operations, '*within which a law enforcement authority collects, processes and analyses information about crime or criminal activities*'.[126] While the access to information stored in the AWF's is principally purpose oriented, it is noteworthy that a single overlap with data that is already processed within another focal point or target group counts as a 'motivated consultation' that might give access to the data stored in these other focal points or target groups, giving automatic output the same investigative justification value as traditional investigative

[120] Ibid., p.96-7, Art. 51
[121] Europol, 'Data Processing at Europol – Who, Where and How?', available at: https://www.europol.europa.eu/st/DPO/#/methods_and_means
[122] Europol, 'New AWF Concept - Guide for MS and Third Parties' (2012), available at: http://www.statewatch.org/news/2013/jan/europol-awf-new-concept.pdf
[123] Ibid. For suspects and convicted persons, potential criminals and contacts and associates, an extensive set of data may be processed, including economic and financial information, behavioural data and occupation. Personal details, physical appearance and identification means are stored for these groups as well as for victims.
[124] Ibid.
[125] Europol, 'Europol Analysis Projects', available at: https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects. Note here that the former focal point on the TFTP has been abolished in comparison to Ibid. above
[126] Europol, *supra* note 122

leads.[127] Taking into account that such cross-matches do not automatically grant the authority to access and analyse the personal data stored in another AP and that the conditions for such use are tailored towards the individual AP profiles, this practice can however still be expected to respect the purpose specification principle.

Intelligence on suspicious transactions is exchanged through national Financial Intelligence Units (FIU) and the transatlantic Terrorist Finance Tracking Program. FIUs act as a decentralised network in which the national unit might occasionally request the assistance of its counter-part in another Member State during its investigation. Therefore, intelligence exchange occurs mainly among member states, although Europol can occasionally serve as a hub and can provide additional criminal information if it is necessary for the national investigation.[128] Meanwhile, the Terrorist Finance Tracking Program is an instrument of the United States that analyses financial messages data sent through the network of the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[129] Since this data is located on European Soil, an agreement for its transfer has been concluded between the EU and the US that assigns a vetting role to Europol, which will be explained in more detail in chapter five.

3.2.4. THE EUROPEAN COUNTER TERRORISM CENTRE

Following a series of terror attacks within the EU, the European Counter Terrorism Centre was established by the EU Justice and Home Affairs Ministers in November 2015 as an information sharing and operational cooperation platform in regard to foreign terrorist fighters, illegal firearms tracking and terrorist financing.[130] It builds on the existing structures of Europol and therefore has access to the AWF's and their relevant focal points, the TFTP, the European Bomb Data System and the network of FIUs. Given its function as a hub of such existing structures, the ECTC was not given an own regulatory framework and therefore operates on the ground of Europol's normative base. The Commission currently plans to enhance the capabilities of the ECTC by further enhancing Europol's access to other EU databases, aiming to strengthen Europol's internal governance and further develop the cooperation with third countries.[131] The

[127] Cf. Ibid.
[128] Europol, 'Financial Intelligence Units – FIU.net', available at https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net
[129] A. Amicelle, 'The Eu's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance,' *Liberty and Security in Europe* 2013
[130] Council of the European Union, 'Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism', available at: http://www.consilium.europa.eu/en/press/press-releases/2015/11/20-jha-conclusions-counter-terrorism/
[131] European Commission, 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders' (2016), available at: http://statewatch.org/news/2016/sep/eu-com-security-mobility-info-exchange-com-602-final.pdf

databases concerned are the Schengen Information System, a governmental database in which information on wanted or monitored individuals is stored, the EU Visa-Information System, which stores information and biometrics on third country nationals who apply for a Schengen Visa, national Passenger Name Record databases of Member States and the European Dactyloscopy (Eurodac), the central fingerprint database for asylum seekers of the EU. Noteworthy is also the proposal to establish links with the Counter Terrorism Group (CTG) of the Club de Berne, opening it for interaction with Member State cooperation conducted within the Europol framework.[132]

3.3. LEVEL OF PROTECTION AND CONSISTENCY WITH FUNDAMENTAL RIGHTS

The exchange of intelligence within the AFSJ, mainly facilitated through the hub of Europol, is governed by an extensive set of primary and secondary legislation. Europol itself describes its data protection regime as 'one of the most robust data protection frameworks in the world of law enforcement'[133], a narrative that has also been reproduced in academic reception.[134] It can indeed be stated that the institution has been given a comprehensive normative framework in which the protection of personal data has been carefully considered regarding data processing actions. Issues like the automatic cross-matching of data with operations carried out within another focal point or the automatic upload of data from national databases to Europol do however raise the question if the legal commitment to data protection is fully implemented in the exchange and analysis activities of EU institutions. While the former is rectified through the limitation of the access to the cross-matched data, the latter raises the question to what extent an algorithm should decide about the onward transfer of personal data. While additional information is needed to further evaluate this issue, suffice it here to state that this practice at least in principle sits uncomfortable with the prohibition of automatic decision making and, potentially, the purpose specification principle.

Despite noteworthy data protection achievements, such as the extensive source verification requirements or the strict rules regarding onward transfer to third countries, the general framework of intelligence exchange within the AFSJ still leaves a variety of questions open that relate to judicial protection and interoperability. First, the problematic situation of judicial

[132] Ibid. The Club de Berne is an informal grouping of the intelligence agencies of the 28 EU Member States, complemented by Norway and Switzerland. Its counter terrorism group is an informal forum for intelligence exchange that was established in 2002.
[133] Europol, 'Transparency', available at: https://www.europol.europa.eu/about-europol/transparency
[134] D. Drewer and J. Ellermann, 'May the (Well-Balanced) Force Be with Us! The Launch of the European Counter Terrorism Centre (Ectc),' 32 *Computer Law & Security Review* 2016,195-204.

protection that arises from Art. 276 TFEU deserves consideration. Since the Court of Justice is explicitly excluded from reviewing the validity or proportionality of national operations that aim at safeguarding internal security and the maintenance of the rule of law, a judicial protection gap can be assumed. It is possible to assume that intelligence that was obtained in a way that might be considered unlawful in regard to privacy and data protection rights if it was brought up to the CJEU is exchanged through instruments of the Union, for example Europol databases. While the subsequent processing of the data might occur in full respect to the data protection framework of criminal intelligence exchange, the way of acquisition would have tainted the legality of the data from the start. Although the Europol Regulation states that '[a]ny information which has clearly been obtained in obvious violation of human rights should not be processed'[135], no operational safeguard was implemented to enable an enforcement of this commitment. In this regard, Directive 2016/680 can be regarded as a major step ahead in safeguarding the rights of individuals in a data fusion environment, as the defining of common rules for the processing and collection of criminal information provides for an effective and feasible solution to the problems of judicial review and interoperability. Rather than pursuing a top-down approach in which the CJEU would need far reaching access to the proceedings of national law enforcement agencies, which could potentially infringe Article 72 and 4 TFEU, the new common rules will ensure in principle that all information that is collected by the relevant authorities fulfils a common European standard. This in turn reduces the danger of tainted information circulating within Europol's systems, as the legality of the personal data that is transferred would be guaranteed by the common rules on collection and the monitoring of the national courts.[136] A common standard also rectifies the potential problems that methods of data collection used in one Member State might not be lawful in another Member State and that individuals might be disproportionately monitored because of their nationality. On the other hand, the Directive only applies to activities conducted within EU law, therefore the protection gap referred to earlier cannot be considered to be fully closed

A remaining issue is the challenge raised by interoperability. While the merging and linking of different databases is on the heart of the intelligence fusion process and a necessity to its success, the process has also alarmed civil liberties groups ever since the first fusion centres were established.[137] In the EU, where interoperability is defined as the '*ability of IT systems and of the*

[135] *OJ* [2016] L 135/58, 24.5.2016, Recital 39
[136] The motive to limit this potential problem can be found inter alia in the Recitals 7, 15 of the Directive 2016/680, *OJ* [2016] L 119/105, 4.5.2016
[137] D.L. Carter and J.G. Carter, *supra* note 3

business processes they support to exchange data and to enable the sharing of information and knowledge',[138] the concept is increasingly promoted in the exchange of counter terrorism information.[139] The definition of interoperability as a solely technical issue attracted fierce criticism that pointed towards the serious political and legal implications of interlinking different databases, especially in the realm of criminal investigation.[140] The main problems are the shifting of intelligence that was gathered for a specific purpose to another area and the eradication of the traditional line between police forces and secret services; In the analysis of Hert and Gutwirt, '*the worst of both worlds are brought together*' when interlinking such actor's respective databases.[141] An 'imperative of separation' (*Trennungsgebot*), which is a for example a constitutional principle in Germany, becomes nonetheless unfeasible in Europol's databases which involve a high number of stakeholders from countries with different constitutional backgrounds and models of law-enforcement. Since some national institutions such as the Finnish Suojelupoliisi or the Estonian Kaitsepolitseiamet have no tradition of separating intelligence and police services, such distinction is rendered impossible on an EU level as well if effective information exchange between all Member States is to be sustained.

The structure of the Europol database systems can be seen as a rectification approach to the interoperability challenge, as it establishes the purpose specification principle and gives Member States a high amount of control over the access to their uploaded data in the EIS. However, some challenges remain, especially regarding the plans to further enlarge Europol's databases by giving it access to other hubs of personal data. While the Schengen Information System does at least have the purpose of fighting crime and therefore also terrorism, the access to other databases is much more problematic Access to the Visa Information System and EuroDac, for instance, would give the institution insight into the biometric data of millions of third country nationals and asylum seekers, especially the latter being a population that is in a special need of protection. Meanwhile, linkages with the ECG might lead to a higher danger of 'tainted' information within Europol's systems because the data protection guidelines of the EU do not apply within the informal circles of the Club de Berne. Finally, the encouraged accessing of national PNR data is questionable because of the nature of the data as such, as it stores the flight and travel data without

[138] Commission of the European Communities, 'Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs' (2005)
[139] European Commission, *supra* note 131
[140] P. De Hert and S. Gutwirth, 'Interoperability of Police Databases within the Eu: An Accountable Political Choice?,' 20 *International Review of Law, Computers & Technology* 2006,21-35.
[141] Ibid.

reasonable suspicion. Access to all of these databases would therefore need to be carefully regulated and tightly limited to prevent a general suspicion of '*suspect communities*'.[142]

It can therefore be summarised that the regulatory framework for non-military actors does recognise and address the challenges raised by intelligence exchange, but also that in order for these measures to fulfil their purpose of full compliance with the human rights and data protection standards as outlined in Chapter 2, additional and continuous effort will need to be made. Having analysed the regulatory peculiarities of the data protection standards for non-military actors, the question remains how the issue of fundamental rights is addressed in legislation directed at military actors. The following Chapter will therefore provide a respective analysis.

[142] C. Murphy, *supra note* 26, describes the phenomenon that through the use of new technologies, 'risky groups' are identified and subjected to an increased level of pre-emptive surveillance. These groups are often highly vulnerable parts of society, such as migrants or refugees.

4. THE REGULATORY FRAMEWORK FOR MILITARY ACTORS

As mentioned earlier, the exchange of counter terrorism intelligence is conducted not only among police authorities, but also among military actors in the framework of the CFSP. This chapter reviews the regulatory framework for such exchanges among Union bodies and Member States, starting with a review of both primary and secondary legislation. It then goes on with discussing this framework in the light of the information that is available on the implementation and execution of counter terrorism intelligence exchanges among military actors.

4.1. PRIMARY LAW PROVISIONS

In comparison to the mandate given to non-military actors by primary law, the competence for counter terrorism intelligence for the CFSP and CSDP is not as expressly provided. The statement that '*Member States shall consult one another within the European Council and the Council on any matter of foreign and security policy of general interest in order to determine a common approach*' (Art. 32 TEU) does not provide for a formalised exchange of intelligence outside the council sphere, neither does the limited statement on the EEAS (Art. 27 (3) TEU), which merely provides that

'[t]his service shall work in cooperation with the diplomatic services of the Member States and shall comprise officials from relevant departments of the General Secretariat of the Council and of the Commission as well as staff seconded from national diplomatic services of the Member States.'

Nonetheless, the CFSP provisions of the TEU are open enough to allow for the establishment of intelligence exchange. The provisions on the tasks of the Union to preserve peace and international security (Art. 21, (2 c) TEU), identify questions of general interest and achieve increasing convergence of Member State Action (Art. 24 (2) TEU), as well as the obligation for Member States to enable the assertion of the Unions interest in the international sphere through convergence of their actions (Art. 32 TEU), can be read to allow for integrative security cooperation, including the establishment of intelligence exchange if it is considered to be a general interest. Additionally, the provisions on the common security and defence policy state that the EU should be equipped with an operational capacity for missions outside of Union territory, including both civilian and military assets that shall be made available by the Member States (Art. 42 (1, 3) TEU). The fight against terrorism is further mentioned as the only specific aim of the tasks that are set out in Art. 43 and may include:

'joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation.'

As intelligence cooperation can be seen as a form of military assistance and advice, the TEU does therefore not pre-empt the Union from taking such measures, however it should be carefully noted that missions that are developed within the CSDP framework need to be carried out outside the Union (Art. 42 (1) TEU). This limitation is of particular relevance for institutions that are established under the framework of the CFSP but also address internal security threats, as analysed in the subsequent sections.

Judicial protection by the CJEU is ruled out by Art. 275 TFEU, which excludes the CFSP and all respective acts from the jurisdiction of the court. However, the Court can give an opinion on the compatibility with the Treaties, and an agreement may not enter force if the Court decides adverse (Art. 218 (11) TFEU). Furthermore, restrictive measures that are of direct concern to an individual may be reviewed regarding their legality by the court (Art. 275, in conjunction with Art. 263 TFEU), which offers the possibility to judicially safeguard fundamental rights of individuals. This provision constitutes an opportunity the court has been noted to use in particular in regard to the right of access to information and the right of access to Justice,[143] which in turn relate to the transparency and judicial protection safeguards that have been identified as highly important for the fundamental rights of privacy and data protection earlier in this study.

4.2. INTCEN, THE EUROPEAN MILITARY STAFF AND THE SINGLE INTELLIGENCE ANALYSIS CAPACITY

The EU Intelligence Analysis Centre was launched in 2002, then called EU Situation Centre (EU SITCEN). In the first days of the predecessor of the CSDP, the European Security and Defence Policy, the institution was originally situated in the council secretariat together with the EU Military Staff.[144] The institution was, however, not rooted in any kind of establishing act until the creation of the European External Action Service that followed the entry into force of the Treaty of Lisbon by Council Decision 2010/427/EU. INTCEN regards itself as '*the exclusive civilian intelligence function of the European Union'*[145] and is staffed by analysts that are

[143] C. Eckes, 'Common Foreign and Security Policy: The Consequences of the Court's Extended Jurisdiction,' 22 *European Law Journal* 2016,492-518.
[144] J.v. Buuren, *supra* note 17
[145] European External Action Service, 'EU INTCEN Factsheet' (2015), available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160615factsheetintcen_/sede160615factsheetintcen_en.pdf

typically dispatched by national intelligence services.[146] Together with the Intelligence division (INTDIV) of the European Union Military Staff (EUMS), it forms the Single Intelligence Analysis Capacity (SIAC), a framework in which both institutions produce joint intelligence products. Because of this cooperation, the fusion centre has been repeatedly described as an institution that bridges non-military and military capacities[147]. INTCEN was tasked with terrorism related monitoring activities and threat assessments since its creation, a mandate that was originally solely focused on the Union's external sphere but that soon expanded into covering internal threats following the Madrid Bombings in 2004.[148] The EUMS intelligence division is, similarly to INTCEN, staffed by national officers who are in this case dispatched by the national military intelligence agencies.[149] The measures conducted within INTCEN and the SIAC, their normative framework and their democratic accountability have been noted by numerous scholars to be highly dubious,[150] a conclusion that is supported by the following analysis.

4.2.1. NORMATIVE FRAMEWORK AND DATA PROTECTION PROVISIONS

Council Decision 2010/427/EU, establishing the EEAS, serves as a legal base for INTCEN as the legal successor of the Joint Situation Centre.[151] The predeceasing institution is only briefly mentioned in Art. 4 (3a) thereof, which provides that the Joint Situation Centre shall be placed under direct authority and responsibility of the High Representative and

'*shall assist him/her in the task of conducting the Union's CFSP in accordance with the provisions of the Treaty while respecting, in accordance with Article 40 TEU, the other competences of the Union*.'

Regarding data protection, the decision refers to Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[152] While the problem that this legislation essentially excludes activities that are conducted wholly within the CFSP from its scope has been

[146] M. a. K. D. Cross, 'A European Transgovernmental Intelligence Network and the Role of Intcen,' 14 *Perspectives on European Politics and Society* 2013,388-402.
[147] See Cross, ibid., den Boer, *supra* note 2 and van Buuren, *supra* note 17
[148] Van Buuren, *supra* note 17
[149] B. M. Müller-Wille, 'For Our Eyes Only? Shaping an Intelligence Community within the Eu. ,' 50 *Occasional Paper* 2004
[150] See Cross, *supra* note 146, den Boer, *supra* note 2 and van Buuren, *supra* note 17
[151] European External Action Service, *supra* note 145
[152] Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service, *OJ* [2010] L 201/38, 3.8.2010, Art. 11 (3)

noted, the resulting legal tension is regarded to be reconciled by the universal validity of Art. 8 CFREU throughout the EU legal order.[153] The provisions on data quality and lawfulness of processing of Regulation 45/2001 are largely consistent with Directive 95/46/EC, the former even being slightly more tilted towards the rights of the data subject.[154] The relevant provisions are further largely consistent with the General Data Protection Regulation of 2016, though the latter has introduced further specifications for the lawfulness of processing.[155] The responsibility for transfers of personal data within or between Union bodies lies both with the controller and the recipient and the transfer legitimacy is dependent on the necessity for the task performance of the recipient.[156] The protection level of special categories of data is again consistent with the former and current data protection directive, including the requirement that data that relates to offences, criminal convictions and security measures may only be processed if it is authorised by primary or secondary Union law, or in special cases by the EDPS.[157] Furthermore, extensive rights of information access, rectification, erasure and blocking are granted in the Directive.[158] A data protection officer shall be appointed and processing operations that are likely to interfere with individual rights are to be checked by the EDPS before the processing occurs.[159]

The implementing rules of these provisions for processing activities carried out by the EEAS were established by the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection.[160] It contains a wide set of provisions on the duties, tasks and powers for the internal EEAS DPO, including for example the ensuring of the implementation of the Decision and the right to initiate investigations in data protection measures, but also the obligation to not 'divulge' information or documents

[153] S. Blockmans et al., 'Eeas 2.0: A Legal Commentary on Council Decision 2010/427/Eu Establishing the Organisation and Functioning of the European External Action Service (February 7, 2013).' *CEPS Paperbacks* 2013 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2213790. The scholars pointed out additionally that activities that are only partly conducted within the CFSP are covered by the Regulation 2010/427/EU due to the provisions of Art. 3 (1) thereof.

[154] Note that the rather vague provision on the legitimacy of processing that is 'necessary for the for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed' (*OJ* L 281 /40 Art. 7f) is absent in the Regulation

[155] The added value of the General Data Protection Regulation compared to the Regulation on the processing of personal data by community institutions lies mainly in its specification that processing carried out in the public interest or for compliance with a legal obligation must be based on Union law and in the provision of criteria for the controllers decision on cases in which no such law is present. *OJ* [2016] L 119/36-37, 4.5.2016, Art. 3, 4

[156] Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ* [2001] L 8/6, 12.1.2001, Art. 7

[157] Ibid., p.8, Art. 10 (5)

[158] Ibid., p.9-11, Art. 12-16

[159] Ibid., p.13-15, Art. 24-27

[160] Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection, *OJ* [2012] C 308/8, 12.10.2012

gained in his/her tasks.[161] All controllers are responsible to comply with the High Representative's decision, which includes the implementation of appropriate technical and organisational safeguards to ensure confidentiality and security of the processing.[162] The right to information is covered by the right to access the register in which the DPO logs all data processing operations and the rights of access, rectification and blocking are provided for by pointing towards the relevant Articles of Regulation 45/2001.[163] An important exception for the exercise of these rights is the limitation posed by Art. 20 (1 a) thereof, which provides that in a case where '*the prevention, investigation, detection and prosecution of criminal offences*' needs to be safeguarded, the rights of the data subject may be restricted.[164] It further prevents the application of the provisions on data quality, which makes fair and lawful processing for a specified and legitimate purpose no longer a requirement as soon as the data is used in a criminal investigation.

Meanwhile, the legal base of the EUMS is found in the Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union.[165] It's mission is the early warning, situation assessment and strategic planning for the Petersberg Tasks, a mandate that is repeated regarding its assigned role, tasks and function.[166] It is further expressly tasked with monitoring '*potential crises by relying on appropriate national and multinational intelligence capabilities*', supplying the Situation Centre with military information as well as with receiving its output.[167] In its original legal base, there is neither a provision on data protection nor a reference to secondary legislation that would have binding force for the EUMS. Since it is, however, placed under the direct authority of the High Representative and is therefore a formal part of the EEAS,[168] the data protection provisions outlined above should apply in principle.

4.2.2. COUNTER TERRORISM DATA EXCHANGE ACTIONS

INTCEN and the EUMS receive and analyse

'information provided by Member States' security and intelligence services, open sources (media, websites, blogs etc.), diplomatic reporting, consular warden networks, international

[161] Ibid., p.8-9, Art. 3-7
[162] Ibid., p.10, Art. 9
[163] Ibid., p.11-2, Art. 15-20
[164] Ibid., p.12, Art. 24 (1) in conjunction with *OJ L* 8/11, Article 20 (a)
[165] Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union, *OJ* [2001] L 27/7, 30.1.2001
[166] Ibid., p.8, Annex 2-4
[167] Ibid., p.9, Annex 4
[168] *OJ* [2001] L 201/33, 3.8.2010, Art. 4 (3 a)

organisations, NGOs, CSDP missions and operations, EU Satellite Centre, visits and field trips'.[169]

Information is also received from Europol for the conduction of internal threat assessments,[170] and the Club de Berne[171] counter terrorism group provides INTCEN with further strategic and threat analyses.[172] It has been stated that the Council used to maintain a strict division between the civilian intelligence dimension addressed by INTCEN and the military intelligence dimension addressed by the intelligence division of the EUMS, respective intelligence of both domains being received and processed only by the particular institution that was tasked to do so.[173] As it has been evaluated earlier, however, this distinction is regarded to be widely overcome by the emergence of the SIAC. While there is little information available on the substantial nature of the information that is processed in the INTCEN-EUMS nexus, some general observations have been made by scholars. Firstly, the intelligence received by INTCEN from national security services comes in the form of national assessments rather than raw intelligence and the decision on which information is passed through depends solely on the national experts.[174] Therefore, INTCEN is unlikely to receive personal data as such from the national intelligence services. Personal data could, however, potentially be received through data that is shared by the Union Delegations or the increasing amount of open-source intelligence that is gathered by INTCEN.

The data processed in the EUMS INTDIV compiles reports from intelligence provided by the national military intelligence agencies with a focus *'on the military capabilities and on how, and respectively by whom, they are controlled in regions of potential and existing crisis.'*[175] Whether such assessments contain personal data and if so, the types of data and their scope are unclear.

4.3. LEVEL OF PROTECTION AND CONSISTENCY WITH FUNDAMENTAL RIGHTS

It can be summarised that the normative framework of INTCEN does not provide for a consistent regulatory framework regarding the protection of fundamental rights. Further, the security nexus posed by INTCEN and the EUMS does again raise the question of interoperability.

For INTCEN, the inconsistency begins already with its mandate, as there is no legal basis for it to cover the internal dimension of the European Union. This shortcoming can be explained by

[169] European External Action Service, *supra* note 145
[170] D. Keohane, 'The Absent Friend: Eu Foreign Policy and Counter-Terrorism,' 46 *JCMS: Journal of Common Market Studies* 2008,125-146.
[171] See explanation in note 132
[172] J.v. Buuren, *supra* note 17
[173] E. R. Hertzberger, 'Counter-Terrorism Intelligence Cooperation in the Eu,' *European Foreign and Security Studies Policy Program UNICRI* 2007
[174] M.D. Boer, *supra* note 2
[175] B. Müller-Wille, *supra* note 149

the history of the fusion centre, as it first emerged without a specific legal basis and task description and was therefore able to be shaped in full accordance with the vision of then High Representative Javier Solana.[176] While the assignment of the fusion centre to the EEAS and the respective normative foundation can be regarded as a first step towards a higher legitimacy, the move also created a new legal paradox by placing the institution solely within the realm of the CFSP. Any action or investigative measure taken by INTCEN since Council Regulation 2010/427/EU entered force and that relates to counter terrorism threat assessment within rather than outside the Union therefore sits highly uncomfortable with Title V of the TEU, as the CFSP is continuously framed as Union action on the international scene and foreign policy (Art. 21, 23, 24 (1) TEU). This might be partially rectified by the provision that the CFSP may cover '*all questions relating to the Union's security*' (Art. 24 (1) TEU), however whether this clause teleologically includes EU internal exchange of counter terrorism intelligence remains questionable to some degree. The same applies in principle to the EUMS as soon as the joint analysis operations conducted in the SIAC cover internal threats.

Regarding the protection of personal data and fundamental rights, both institutions are in principle covered by the data protection provisions of the EEAS and are therefore consistent with the general protection framework regarding data transfers between Union bodies. Nonetheless, it is argued here that this framework is neither sufficient for the security related tasks of the institutions nor for the protection of individuals. First, the High Representative Decision, in conjunction with Regulation 45/2001, poses heavy restrictions to the protection of personal data in criminal matters. As processing operations carried out by INTCEN and INTDIV address internal security and counter terrorism, the regulation is therefore unlikely to unfold any protective effect. Given that the two fusion centres are composed of national officers who serve as a link to their respective Member State agencies, it is further highly unlikely that the EEAS DPO can exercise his/her scrutiny regarding the transfers conducted within these structures in the same way he/she does in other EEAS areas. The fact that the regulatory environment in which the institutions operate is therefore completely inept for public security related transfers poses a stark contrast to the non-military framework in which Europol conducts its exchanges.

The absence of more task specific rules for INTCEN and the EUMS INTDIV surely stems primarily from the great secrecy that surrounds the institutions, which is fostered by both the Member States as well as the institutions themselves and that shields them from public scrutiny

[176] Cf. J.v. Buuren, *supra* note 17

and accountability.[177] Moreover, the European intelligence community and therefore the exchange of data among its institutions suffers from a chronic lack of trust,[178] which might have substantially reduced the incentives for establishing oversight and rules for a cooperation that was already regarded to be insufficient. Nonetheless, an additional explanation may be found in the nature of the processed data: The reliance on ready assessments from the Member States intelligence agencies or the Berne CTG might raise fewer concerns regarding the protection of personal data than an actual transmission of raw intelligence would do, especially since such products might relate more to general trends and developments in the area of terrorism than to the monitoring of specific individuals. The same could apply to information transferred by Europol or the Union Delegations. However, this cannot serve as an excuse for the absence of a coherent normative framework because of two reasons. First, it cannot be ultimately verified that the above statement is actually true and that indeed, no intelligence that involves personal data or that was conducted in a way that violates the rights of individuals is processed in the SIAC. Secondly, even if no such data is transferred at this point in time, the absence of a regulatory framework for intelligence exchange means that there is no guarantee that exchanges of personal data might occur in the future, especially given that the history of INTCEN is featured by various task expansions that were not provided for by law. The rather unfitting regulatory framework could further constitute an obstacle for the judicial protection of individuals, especially since the secretive nature of the mostly intergovernmental measures taken within INTCEN and INTDIV prevents a deeper assessment to what extent individual rights could potentially be violated, which in turn makes it unlikely that restrictive measures could be reviewed by the CJEU.

It can therefore be summarised that the regulatory framework for military actors regarding counter terrorism intelligence exchange is unfitting with the constitutional principles of the Union in two dimensions, scilicet through internally oriented monitoring by CFSP institutions as well as through the absence of a regulatory framework for the exchange of criminal investigation and security related information. While it cannot be ultimately determined whether the fundamental rights of privacy data protection are violated by INTCEN or INTDIV, the regulatory framework for military actors therefore certainly sits uncomfortable with the principle of a community based on the rule of law. The current regulatory status quo is of course the product of a gradual non-linear security integration and the challenges raised by international terrorism on the one side and a European community which is unified in regard to free movement, but

[177] Cf. M.a.K.D. Cross, *supra* note 146. The author holds inter alia that INTCEN intentionally keeps a low profile to earn more trust from Member State intelligence agencies.
[178] D. Keohane, *supra* note 170, and M.a.K.D. Cross, *supra* note 146

fractured in its intelligence architecture on the other. Therefore, it would be unjustified to apply the same standards of sophistication and protection of individuals that are expected from national intelligence services to the CFSP's civilian and military intelligence divisions. However, the potential dangers of an unregulated intelligence community should also be duly noted,[179] and several improvements could be made. The High Representative could, for instance, amend the existing EEAS Decision on data protection to include clauses that more adequately address data protection for security purposes, or even draft a second Decision specifically targeted at the intelligence exchange actions of INTCEN and INTDIV. Inter alia, such decisions could regulate what type of data is exchanged, what safeguards apply when this data includes personal information, the conditions under which civilian and military data may be merged in the SIAC and what Treaty Provisions are considered to be the adequate basis to cover EU internal threat assessment. Other proposals have named the establishment of an independent intelligence oversight body.[180] Such specifications would significantly increase the normative coherence and the transparency of the intelligence institutions that are subordinated to the EEAS without infringing their current work. From a long-term perspective, it might also be beneficial to consider disentangling the internal and external dimension again, which would require INTCEN to solely focus on external intelligence and the movement of internal analysis capacities to a newly formed internal intelligence service – whose tasks would then again need to be clearly distinguished from the ones covered by Europol. Whether such a mirroring of the intelligence setup of most Member States is likely or desirable remains to be seen, the first step should, however, be to begin the rectification of the regulatory problems and inconsistencies pointed out in this section.

This Chapter closes the analysis of the regulatory framework and intelligence exchange actions of relevant EU counter terrorism actors. As such exchanges are, however, not only conducted within the Union, but also with third countries, the following chapter will address the external dimension of EU counter terrorism intelligence exchange.

[179] A detailed analysis of the peculiarities of democratic accountability in the realm of intelligence services can be found in J. van Buuren, *supra* note 17
[180] M. D. Boer, *supra* note 2

5. COUNTER TERRORISM INTELLIGENCE EXCHANGE IN EU EXTERNAL AGREEMENTS

This Chapter reviews the external dimension of EU counter terrorism intelligence exchange. After evaluating the primary law provisions for such exchanges, the most relevant agreements with third countries as well as relevant EU military missions are introduced and their respective regulatory provisions are reviewed in regard to their consistency with internal human rights and data protection standards.

5.1. PRIMARY LAW PROVISIONS

The competence to conclude international agreements is expressly conferred to the Union by Art. 216-218 TFEU. Rather than listing specific contents of such agreements, Art. 216 TFEU externalises the internal competences of the Union by providing that agreements may be concluded

'where the Treaties so provide or where the conclusion of an agreement is necessary in order to achieve, within the framework of the Union's policies, one of the objectives referred to in the Treaties, or is provided for in a legally binding Union act or is likely to affect common rules or alter their scope'.

For non-military actors, the treaty provisions that enable a common definition of terrorism, the establishment of measures directed at promoting and supporting crime prevention action of Member States, the establishment of common rules for the collection, storage, processing, analysis and exchange of relevant information the establishment of common investigative techniques for Member States' law enforcement agencies (Art. 83, 84, 87 (1 a, c) TFEU) therefore unfold an external dimension on this ground. Similarly, Europol's expressly provided task to collect, store, process, analyse and exchange information implies a clear treaty provision for intelligence exchange with third countries, which was further codified in Article 25 of its regulatory framework.[181]

For the CFSP, the provisions on the tasks of the Union to preserve peace and international security (Art. 21, (2 c) TEU), identify questions of general interest and achieve increasing convergence of Member State Action (Art. 24 (2) TEU), as well as the provisions on the obligation for Member States to enable the assertion of the Unions interest in the international

[181] Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ* [2016] L 135/53, 24.5.2016

sphere through convergence of their actions (Art. 32 TEU) have an explicit external dimension and provide legitimacy to the conclusion of respective external agreements, especially since the CFSP has an additional provision for the conclusion of external agreements in Art. 37 TEU. Given this holistic, rather vague approach towards the Union's security, the CFSP Treaty provisions can be expected to include counter terrorism intelligence exchange if it is identified as a common interest of the Union's members.

5.2. COUNTER TERRORISM INFORMATION EXCHANGE CLAUSES IN EU EXTERNAL AGREEMENTS AND MILITARY MISSIONS

A variety of EU agreements with third countries as well as some Council joint actions that establish EU military missions include express provisions on counter-terrorist information sharing, or provisions that imply the possibility for such exchanges. Depending on the level of cooperation these agreements establish, their operational arrangement as well as the inclusion of data protection provisions varies. What further complicates the assessment of data protection implications that might arise from the specified information exchanges in the analysed agreements and missions are the vague definitions of the type of information that is exchanged. Where information on '*terrorist groups and their support networks*' shall be exchanged, no further definition is given on the exact types of data that might be concerned. When EU classified information is to be exchanged, the extent to which this might include personal data is equally unclear. The Council definition of classified information as any information '*the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States*'[182] is in principle open to include personal data.

Table 1 below provides an oversight of existing EU agreements that have a counter terrorism intelligence exchange dimension. Additionally, CSDP military missions that might also include the sharing of information have been considered.

[182] Council Decision of 23 September 2013 on the security rules for protecting EU classified information, *OJ* [2013] L 274/2, 15.10.2013, Art. 2 (1)

Table 1

	Express Counter-terrorism clause	**Counter-terrorism intelligence exchange clause**	**Clauses on the protection of personal data**
Stabilisation and Association Agreement With Albania, OJ 28.04.2009 L107 p.166	**Article 5** The Parties reaffirm the importance that they attach to the fight against terrorism and the implementation of international obligations in this area. **Article 84** Counter-Terrorism	**Article 84** by exchanging information on terrorist groups and their support networks in accordance with international and national law;	**Article 73 (3)** Approximation of laws, including data protection **Article 79** Harmonisation of Albania's legislation concerning personal data protection with Community law and other European and international legislation and establishment of independent supervisory bodies.
Stabilisation and Association Agreement with Serbia, OJ 18.10.2013 L278, p.16	**Article 7** The Parties reaffirm the importance that they attach to the fight against terrorism and the implementation of international obligations in this area. **Article 87** Combatting terrorism	**Article 87** by exchanging information on terrorist groups and their support networks in accordance with international and national law	**Article 81** Harmonisation of Serbia's legislation concerning personal data protection with Community law and other European and international legislation and establishment of independent supervisory bodies.
Euromed Agreement with Algeria OJ 10.10.2005 L265, p. 2	**Article 90** Fight against terrorism	**Article 90** through the exchange of information on terrorist groups and their support networks in accordance with international and national law	
Euromed Agreement with Egypt, OJ 30.09.2004 L304/39	**Article 59** Fight against terrorism	**Article 59** exchange of information on means and methods used to counter terrorism	
Partnership and Cooperation Agreement Iraq, OJ 11.05.2012 L 204 (undergoing ratification)	**Article 4** Combating terrorism	**Article 4** by exchange of information on terrorist groups and their support networks in accordance with international and national law	**Article 104** Cooperation commitment to improve level of personal data protection to highest international standards, cooperation may include technical assistance
Partnership and Cooperation Agreement Tajikistan OJ 29.12.2009 L350, p.3	**Article 71** fight against terrorism	**Article 71** by exchanges of information, in accordance with the international and national laws on terrorist groups and their support networks	
EU – Central America Political Dialogue And Cooperation, OJ 15.04.2014, L 111/6	**Article 3 (2)** Objectives; inter alia counter-terrorism **Article 50** Cooperation in the field of counter-terrorism	**Article 50** by exchange of information on terrorist groups and their support networks in accordance with international and national law	**Article 35** Cooperate to on the protection of data and promote international standards, improve level of protection with due regard to the domestic legislation of the Parties **Article 58** the Parties agree to accord a high level of protection to the processing of personal and other data, compatible with the highest international standards.

Council Joint Action 2008/ 124 /CFSP establishing EULEX Kosovo, OJ 16.02.2008 (as amended by Council Decision 2012/291/CFSP)	Article 2 (d) **Ensure that terrorism is properly investigated and prosecuted**	Article 18 (1) **Release of EU classified information generated for purposes of EULEX Kosovo to United Nations, NATO/KFOR and other third parties** Article 18 (2) **Release of EU classified information up to level of 'UE RESTREINT' by Secretary General/High Representative to local authorities in an event of immediate operational need**
Council Decision 2012/392/CFSP on the European Union CSDP mission in Niger, OJ L 187/48, 17.7.2012	**Article 1** Establishment of the CSDP mission to support Nigerian security actors to fight terrorism	**Article 15** High Representative may release EU CONFIDENTIAL classified information generated for the purpose of EUCAP Sahel Niger to third states

What becomes apparent regarding the agreements is the consistent formulating of the agreed exchanges, which in all cases except the one of Egypt names the exchange of information on terrorist groups and their support networks in accordance with national and international law. Much more inconsistent, however, is the establishment of data protection rules. The agreements with Albania and Serbia provide for a comprehensive approximation of the countries' privacy and data protection laws. This might also include the approximation of data protection in criminal proceedings, which would ensure that the standard of protection for personal data that would be transferred to these countries would be equivalent to EU internal standards. In comparison, the Euromed and the Partnership and Cooperation agreements concluded with Egypt, Algeria and Tajikistan pose a stark difference in this regard, as data protection provisions are entirely absent from these accords. This might primarily stem from the much closer association of the EU with membership candidate Serbia and potential membership candidate Albania, and it might additionally be argued that the stressing of the accordance of the information exchange with national and international law already provides a significant safeguard. Provided that 'international law' includes EU legislation, the transfer of personal data from Member states would need to comply with Directive 2016/680 and transmissions from Europol's database with Regulation 2016/794.[183] On the other hand, the not yet ratified Partnership and Cooperation Agreement with Iraq includes a commitment to high data protection standards and includes the provision technical assistance to raise the level of protection. This could either mean that more personal data is shared by the EU with Iraq than with the other Euromed or cooperation partners,

[183] Transfers from Member States would be dependent on an adequacy decision of the Commission or the provisions on appropriate safeguards, while Europol could only transfer data on the basis of an adequacy decision, a concluded agreement or a case-by-case authorisation of its Executive Director.

or, taking into account that the Iraq agreement was the latest partnership agreement to be concluded, that data protection provisions are increasingly present in EU agreements that involve the sharing of information. The latter interpretation is potentially supported by the EU-Central America Political Dialogue and Cooperation Agreement, which also features clauses on the commitment to highest international standards of the protection of personal data and on cooperation for respective improvements. Regardless of such clauses, none of the non-association agreements contains a set of rules regarding data protection that is as comprehensive as the EU's internal standard. However, given that the agreements on the other hand also do not implement an operational framework for the exchange of counter terrorism intelligence and given that most of the relevant actors within the EU are bound by internal safeguards, the counter terrorism information exchange clauses are also unlikely to violate the fundamental rights of individuals.

Regarding EU military missions, the only provisions that might be related to counter terrorism intelligence exchanges are those that authorise the High Representative to share classified information with third countries or actors, such as local authorities or the North Atlantic Treaty Organisation (NATO). It is not clear to what extent such classified information might include personal data. The intelligence for the mission purposes is provided by Member States for the strategic planning on site and is therefore unlikely to refer to specific individuals. Moreover, the Council Decisions on the military missions also do not establish institutionalised exchanges of information and can therefore not be expected to violate individual rights.

5.3. CFSP AGREEMENTS ON THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION

The EU has concluded numerous agreements with third countries on the exchange and the protection of classified information on the basis of Article 37 TEU. While those agreements do not serve an express counter terrorism purpose, they establish operational intelligence exchange links with third countries and are therefore briefly discussed in the following.

Agreements on the exchange of classified information have been concluded with 19 countries, including accession candidates such as Moldova or Serbia, neighbouring countries such as Liechtenstein or Russia and allies such as the United States, Canada or Israel. Classified information agreements have further been concluded with three international organisations, scilicet the European Space Agency, the North Atlantic Treaty Organisation and the Organisation for Joint Armament Cooperation. They consistently rule that classified information that is exchanged needs to be protected by a framework of safeguards that provides a level of protection

equal to the one of the originator party. Furthermore, information may only be disclosed to third parties if the originator party gave its consent, and some of the agreements rule out any of such transfers.[184] The purpose specification principle is also present in all agreements, and newer agreements such as the one concluded with Moldova or Georgia contain additional provisions on the access of individuals to the transferred data.[185] An example of the latter is the 'need to know' principle, under which individuals need a specific reason to access classified data rather than having universal access through a security clearance. Regarding the necessary 'equal level of protection' that was referred to earlier, the agreements refer to the Council Decision on the security rules for protecting EU classified information. This decision contains a variety of protection clauses related to personnel security, physical security and the management of classified information,[186] but provisions on the protection of personal data are entirely absent. As mentioned in 5.2, the extent to which classified information contains personal data is unclear, which complicates an assessment of the severity of such a protection gap. Nevertheless, two observations can be noted. First, it can be assumed that the level of protection for personal data that is exchanged in the classified information context is protected equivalent, if not even better, then within other regulatory frameworks discussed in this study. This stems from the reversed institutional logic regarding the protection of the data: While data protection provisions within regulatory frameworks such as the one of Europol are codified based on the motivation to protect individuals from a potentially intrusive public entity, the motivation to protect classified information lies in the protection of the entity itself from potential harm. Therefore, public authorities might see benefits in reducing the level of protection of the former, but might be highly careful to ensure the protection of the latter. However, even if this logic implies that the exchange of and access to classified personal data provides a high level of protection, it leaves open the regulatory gap of the acquisition of the data. As classified information might originate from distinct EU sources, the assurance that no personal data is exchanged that was collected in violation of individuals' fundamental rights is essentially dependent on the streamlining of the different EU regulatory frameworks concerning the safeguards for acquiring and exchanging personal data. Looking at the preceding analyses, this suggests that in the current status quo a high standard of personal data protection is ensured for counter terrorism intelligence that stems

[184] A noteworthy exception is the agreement concluded with the NATO, which allows for the disclosure of transferred data to NATO and EU Partnership for Peace Member States. However, a principle of originator control is established and generic releases of data are prohibited unless operational guidelines have been established that regulate such generic exchange.
[185] See, for instance, the Agreement between Georgia and the European Union on security procedures for exchanging and protecting classified information, *OJ* [2016] L 300/4, 8.11.2016, Art. 5 e-g
[186] *OJ* [2013] L 274/3, 15.10.2013, Art. 7, 8, 9

from police forces and Europol, while no such protection can be assumed for information stemming from national intelligence services and INTCEN.

5.4. BULK DATA SHARING AGREEMENTS IN THE CONTEXT OF FIGHTING TERRORISM

Apart from peer-to-peer data exchange agreements as described above, the Union has also concluded agreements that allow the transfer of bulk data from European soil to the security agencies of third countries. The agreements concerned are the EU-US agreement on the terrorist finance tracking program and the passenger name records agreements that were concluded with the United States, Canada and Australia. In the following, an overview over the respective agreements, their normative provisions and their implications for counter terrorism intelligence exchange will be given.

5.4.1. THE EU-US AGREEMENT ON THE TERRORIST FINANCE TRACKING PROGRAM

The Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program[187] was concluded in 2010 and regulates the transfer of financial payment messages from providers located in the EU to the US Treasury Department, as well as the processing of such data by relevant security actors of the EU and the Member States.[188] The agreement had become necessary after the US Terrorist Finance Tracking Program was disclosed by the *New York Times* in 2006, revealing that copies of financial messages sent through the system of the Society for Worldwide Interbank Financial Telecommunications (SWIFT) had been provided to the US Treasury since 2001.[189] SWIFT is a member owned cooperative of financial institutions and provides the network for approximately 80% of global electronic value transfer.[190] The disclosure provoked a political turmoil among European legislators and data protection authorities, who were concerned about these large data transfers by SWIFT, a company that is located in Belgium and therefore in the domain of EU

[187] *OJ* [2010] L 195/5, 27.7.2010, p.4
[188] Ibid., p.7, Art. 1 (1 a)
[189] E. Lichtenstein and J. Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror', *The New York Times*, 23 June 2006, available at: http://www.nytimes.com/2006/06/23/washington/23intel.html
[190] Council of the European Union, 'Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (June 2007), available at: http://europa.eu/rapid/press-release_PRES-07-157_en.htm

data protection legislation.[191] The agreement that was subsequently concluded with the United States was initially rejected and therefore invalidated by the European Parliament, but was ratified soon after additional privacy safeguards demanded by the parliament were adopted. The resulting normative framework will be discussed in the following regarding its compliance with fundamental rights.

The agreement serves two specified purposes, scilicet the provision of financial data that is stored in EU territory to the US Treasury Department and the sharing of counter terrorism information stemming from the US TFTP with law enforcement, public security or counter terrorism authorities of Member States, or Europol or Eurojust.[192]

The agreement rules that the requests by the US treasury department to obtain data need to be narrowly specified, including as clear as possible specification of the category of data requested, a clear indication of why a transfer is needed and tailoring based on geographic, threat and vulnerability analyses.[193] It is further specified that searches conducted in the transferred data shall be based on concrete evidence that the subject might be involved in terrorist activities, shall be tailored and sensitive towards special categories of data.[194] Important to note here is that neither the scope of the requests nor the conducted searches in the data need to be necessarily targeted towards a specific individual. The operational reality is that the US authority requests are still formulated very broad and cover a period of every single day year after year, through rowing continuous requests every month.[195] The resulting transfer of bulk data that is very wide in material, geographic and timely scope is however not only based on a respective intention of the US Treasury Department, but also on the technical impossibility to provide such highly specified information within the SWIFT operating centres, as the encrypted structure of the SWIFT financial messages apparently completely denies the possibility to monitor the transactions of a single target for a specified time span.[196] This situation is unlikely to meet the requirements that the CJEU has made concerning the legality of data retention: Although the court has recently argued that data retention of groups of persons or geographic areas can be legitimate,[197] the available information on the amount and scope of transferred data suggests that

[191] A. Amicelle, *supra* note 129
[192] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program *OJ* [2010] L 195/7, 27.7.2010, Art. 1 (1)
[193] Ibid., p.8, Art. 4 (2 a, b, c)
[194] Ibid., p.9, Art. 5 (5, 6, 7)
[195] A. Amicelle, *supra* note 129
[196] Ibid.
[197] Joined Cases (C-203/15) and (C-698/15), *Tele2 Sverige AB* v *Post- och telestyrelsen***,** and *Secretary of State for the Home Department* v *Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales* [2016], para. 108

the transferred data might still be too broad to meet the requirements of evidence based target specification. However, as information on the volume of financial data that is transferred is continuously framed as a security risk,[198] it is not possible to fully evaluate this issue.

Oversight regarding the transfer of the data is exercised in two ways. The decision on whether a transfer is authorised lies with Europol, which monitors the compliance of the Treasury's request with the provisions of the agreement.[199] While this gives a noteworthy vetting role to Europol, the setup has been heavily criticised because the organisation determines the necessity of the transfer based on operational considerations and security needs rather than the legal criteria that a judicial body would have applied.[200] Oversight over the searches made by the Treasury analysts within the transferred data is further exercised by independent overseers, including a person appointed by the Commission, who shall have the power to review searches made in the provided data and further the power to block all non-complying searches.[201] In the last period, 27 095 searches were conducted, of which 450 were queried and 45 were considered to be too broad and therefore blocked.[202] Considering the vast amount of carried out searches, as well as the comparatively low number of inquiries and the fact that of the roughly 2 per cent of searches that were monitored, 10% were found to be invalid, scholars have questioned the extent to which the overseers can actually exert meaningful oversight.[203]

The Treasury Department is demanded to annually identify and delete non-extracted data, and further to delete any data that was transmitted without prior request.[204] Concerning onward transfer, the agreement holds that information gained in an individualised search may be shared with law enforcement, public security, or counter terrorism authorities in the United States, Member States, or third countries, Europol, Eurojust or other appropriate international bodies, provided that it contains a lead regarding terrorism.[205] Data transfers shall be logged and the receiving authorities shall delete it as soon as necessary, further the sharing of data with third countries is dependent on the consent of the Member State the suspected individual originates

[198] European Commission, 'Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' (January 2017), available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_swd_en.pdf
[199] *OJ* [2010] L 195/7, 27.7.2010, Art. 2 (4, 5)
[200] A. Amicelle, *supra* note 129
[201] *OJ* [2010] L 195/10, 27.7.2010.10, Art. 12
[202] European Commission, *supra* note 198
[203] C. Murphy, *supra* note 26
[204] *OJ* [2010] L 195/9, 27.7.2010, Art. 6 (1, 2)
[205] Ibid., p.9, Art. 7 (a, b, c)

from.[206] Rights of the data subject, composed by the right to information, access, rectification, erasure or blocking are also codified, however their exercise is dependent on the legal situation of the United States.[207] Their design also differs from internal frameworks regulating information exchange: While the 2008 Framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters for example provides that individuals shall be informed about the recipients of their data and the categories of data that is processed,[208] the TFTP agreement only states that the individuals shall be informed about whether their data protection rights had been respected.[209]

The issues outlined above indicate two major problems in evaluating the compliance of the agreement with the Union's internal human rights and data protection standards. First, the immense secrecy that is exercised concerning the scope and volume of transferred data makes a precise evaluation impossible. This lack of transparency is itself highly problematic and democratic oversight over the agreement's implementation is insufficient, which was highlighted in the unprecedented denial of access to the 2012 implementation report for the European Ombudsman during her inquiry whether that document should be made public.[210] The second major problem is the technical nature of the financial messages data, which apparently does not allow for individually targeted transfers of data. If the resulting bulk of data that needs to be retained would be too broad to comply with the European standard of data protection, this could invalidate the retention of such data altogether. This would strip public security forces of an otherwise valuable monitoring tool, although it has been stated that while the measure works well in the retrospective analysis of a terror attack, the claimed preventive effect has not been proved.[211] This problem also casts a significant shadow over the legitimacy of the currently discussed European TFTP. However, the adoption of such a measure in the internal EU domain also bears the promise of a higher scrutiny towards its exact technical implementation and legal consistency with fundamental rights – which would in turn provide a better factual basis for a more substantive evaluation of the EU-US TFTP.

---

[206] Ibid., p.9-10, Art. 7 (d, e, f)
[207] Ibid., p.11, Art. 15-16
[208] *OJ* [2008] L 350/68, 30.12.2008, Art. 16 (2 a)
[209] *OJ* [2010] L 195/11, Art. 15 (1)
[210] Emily O'Reilly, 'Decision of the European Ombudsman closing the inquiry into complaint 1148/2013/TN as regards Europol LIBE Committee', European Parliament, Brussels, Thursday 8 Jan 2015, available at: http://statewatch.org/news/2015/feb/ep-omb-speech-europol-15.pdf
[211] A. Amicelle, *supra* note 129. In striking similarity to Amicelles argument, all cases presented in the latest review of the TFTP, *supra* note 202, were featured by a use of TFTP information after a terrorist attack was conducted or a person suspected of terrorism was arrested. There is still no information on a case in which the TFTP helped in the preventive identification of a potential terrorist or terrorist network.

5.4.2. THE PASSENGER NAME RECORDS AGREEMENTS

The EU has concluded agreements regarding the transfer of Passenger Name Records with the United States, Australia and Canada. As mentioned earlier, PNR data refers to records of each passenger's travel requirements, including, but not limited to, name, travel date and travel itinerary. Currently, the CJEU is assessing the validity of a new EU-Canada agreement[212] and its ruling could have far reaching consequences not only for the agreements that were already concluded, but also regarding the recently adopted inner European PNR scheme. While the PNR agreements have been justified with the fight against terrorism and provide for the possibility to transfer collected intelligence on to EU Member States, the cooperation and sharing practice is less focused compared to the cooperation in the TFTP and they are therefore less relevant for the context of this study. However, some general remarks on their intelligence exchange provisions and compliance with fundamental rights will be made in the following.

One of the most criticised features of the PNR agreements are their inconsistent retention periods. While the 2006 EU-Canada agreement provides for a maximum of six years of retention[213] and the EU-Australia agreement for a maximum of five and a half years[214], the agreement concluded with the United States allows a retention period of 15 years.[215] These stark differences have led scholars to the conclusion that the retention periods might be based more on political negotiations rather than subjective criteria of necessity.[216] Differences also exist in regard to sensitive data: While the agreement with Australia provides that sensitive data shall be deleted in any case,[217] the US agreement allows the storing and use of such data under special safeguards.[218] On the other hand, the rights of access, information, non-discrimination, rectification and redress have been much more consistently codified in the new agreements compared to previous ones, which can be seen as substantial progress.

Concerning the sharing of information, the EU-US agreement states that analytical information relevant to the prevention or detection of terrorist offences or transnational crime shall be provided as soon as possible to EU Member States authorities, as well as to Europol and Eurojust.[219] The respective authorities shall also be able to make requests for specific data leads,

---

[212] European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice' (Brussels, October 2014), available at: http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice
[213] *OJ* [2006] L 91/49, 29.3.2006, Annex 8
[214] *OJ* [2012] L 186/8, 14.7.2012, Art. 16
[215] Ibid., p.5, 11.8.2012, Art. 8
[216] C. Murphy, *supra* note 26
[217] *OJ* [2012] L 186/6, 14.7.2012, Art. 8
[218] Ibid., p.8, 11.8.2012, Art. 6
[219] Ibid., p.11, Art. 18 (1)

which shall be transferred on a case by case basis provided it meets the definitions given in the agreement.[220] Such terrorism related requests are also possible in the EU-Australia agreement, however interestingly no link to terrorism is required for the proactive sharing of Australian authorities to EU Member States and institutions.[221] While these provisions in principle ensure a transfer of data that is individually tailored to a specific case, it should be noted that there are no provisions that further state what criteria are applied to determine the validity of the request or transfer.

To conclude, it can be stated that while the PNR agreements have made continuous progress in regard to the protection of data and the safeguards concerning intelligence exchange, their protection standards still remain weaker than the ones in the domestic sphere of the EU. As in the case of TFTP agreement, there also remains the fundamental question whether the bulk transfer and retention of personal data is compatible with fundamental rights in the first place, especially in the light of the CJEU's decisions on EU internal data retention. On the other hand, no agreement would leave European airlines operating in the US in a legal limbo, as they would face a situation in which they would have to breach the law of a jurisdiction that demands them to disclose their PNR to comply with the law of another jurisdiction that forbids them to do so and vice versa. The pending judgement of the CJEU concerning the 2013 EU-Canada agreement will hopefully shed more light on this issue.

[220] Ibid., Art. 18 (2, 3)
[221] *OJ* [2012] L 186/6, 14.7.2012, Art. 6

5.5. EUROPOL AGREEMENTS WITH THIRD COUNTRIES

Europol has concluded numerous strategic and operational intelligence exchange agreements with third countries. While strategic agreements involve the sharing of best practices and technical expertise, operational agreements additionally involve the sharing of personal data.[222] The legal basis for exchanging data with third countries and international organisations is found in Article 25 of Europol's regulatory framework.[223] Officially, the exchange of personal data is only conducted in two ways if the third country has adopted the EU's data protection rules and benefiting from Europol's intelligence is not possible if the country has not done so.[224] However, it has been suggested that the extent to which data protection provisions are actually included and enforced in operational agreements strongly depends on the extent of power the EU has regarding vis-à-vis its bilateral partner.[225] Europol has to this date signed operational agreements with 15 countries, scilicet Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, the Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland and the United States of America.[226] In the following, a comparative overview regarding the provisions on rights of the data subject, retention period, purpose specification and onward transfer will be given.

Europol's agreement with third countries have been concluded between 2002 and 2016 and differ in regard to their data protection provisions, although some principles are almost universally present. Regarding the operational setup, all agreements establish a national contact point as the central, yet mostly not only point of contact. In most cases, this is the partner's highest national police authority or a police directorate in the partner's Ministry of the Interior. The agreement partners also commonly detach Liaison Officers, who shall facilitate the exchange of information.[227]

The first operational agreements that involved the transfer of personal data were signed with the European Free Trade Area (EFTA) countries Norway and Iceland in June of 2001. They

[222] E. Ilbiz, C. Kaunert, and D. Anagnostakis, 'The Counterterrorism Agreements of Europol with Third Countries: Data Protection and Power Asymmetry,' *Terrorism and Political Violence* 2015,1-18.
[223] *OJ* [2016] L 135/78, Art. 25
[224] E. Ilbiz, C. Kaunert, and D. Anagnostakis, *supra* note 222
[225] Ibid.
[226] The individual agreements can be retrieved from: https://www.europol.europa.eu/partners-agreements/operational-agreements
[227] In the agreements concluded with Albania, Australia, Bosnia and Herzegovina, the Former Yugoslav Republic of Macedonia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia and Switzerland provide that national officers shall be detached to Europol, while Europol officers might be sent to the partner state if it further facilitates information exchange. Colombia agreed to send Liason Officers, but no provision on the detachment of Europol officers is provided in the respective agreement. The US, Canada and Australia agreements allow for the establishment of Liason Officers if it is logistically feasible.

featured a common blueprint that was later also used for EFTA member Switzerland in 2004. They specifically state the fight against terrorism as one of the objectives of the cooperation. This inclusion might be a direct reaction to the devastating terrorist attacks conducted in the United States in 2001, which is underscored by the fact that the fight against terrorism was only added to Europol's tasks one year after the conclusion of the Iceland and Norway agreements. Regarding the protection of personal data in information exchange activities, they provided that personal data may only be transferred for the investigation of individual cases and that special categories data may only be transferred if definitely necessary. There are further extensive criteria for the reliability of sources of information and all communications shall be logged. Data subjects have the right to access their data or have it checked. Regarding onward transfers, all transmissions are dependent on the consent of the Member State from which the data originates and the communication of data to third states or international bodies is not allowed. The data may, however, be forwarded to other competent authorities that were specified in the agreements, including regional police forces and customs services. Personal data may be retained for a period of three years, which can begin anew if further processing is considered necessary after an obligatory review.

The second operational link was established with the United States, which featured a counter terrorism objective equivalent to the previous Europol Agreements.[228] The supplemental agreement on the exchange of personal data and related information[229], concluded one year after the initial Europol-US agreement to allow for the exchange of personal data, provides that special categories data shall only be transferred if necessary for a criminal investigation, that transmission of personal data shall be conducted for the purpose of fighting crime and the accuracy of the information shall be maintained, the agreement falls short on a variety of data protection principles that are present in later agreements. It does neither include a time period for the retention of the transferred data, nor does it limit the extent to which the data may be processed. There is further no indication other than 'competent US Federal Authorities' regarding which institutions may have access to the personal data.

In comparison, the agreement with Canada[230], concluded in November 2005 with a solely counter terrorism targeted purpose, provided for a higher standard of protection. It ruled that information about the use of transferred personal data shall be made available after receipt and

[228] Agreement between the United States of America and the European Police Office [2001], Art. 3 (1 f)
[229] Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and related Information [2002]
[230] Co-Operation Agreement between the Government of Canada and the European Police Office [2005], *supra* note 226

that the processing of data for a purpose other than the one it was originally transferred for as well as the transfer to a third country of international body is dependent on the transmitting party's consent. It further required an indication of the source of the data and a record of all transfers and receipts of personal data. However, the specific law enforcement institutions that would receive the data were not named and no maximum retention period was established.

The agreement with Australia[231] included most of the above-mentioned features in an improved form, for example through requiring a source assessment of an equal level as the agreements with the EFTA countries. The agreement serves inter alia a counter terrorism purpose, as it covers all areas of crime within Europol's regulatory framework and gives a specific reference to the urgent problem raised by terrorism in its preamble. It included for the first time not only the right of access, but also the rights of correction and deletion for the data subjects in accordance with the respective normative framework. Further, the Australian regional police forces were specified as the only competent national authorities to which the national contact point could forward transferred data. A shortcoming was, however, again the omission of a specified retention period.

Operational agreements with Monaco and the Former Yugoslavian Republic of Macedonia were signed in 2011. Their relation to counter terrorism and their data protection provisions were largely similar with the EU-Australia agreement, but they additionally featured a renewable retention period of 3 years. The agreement signed with Colombia[232] in 2013 again emphasised terrorism in its preamble and covers all areas of crime Europol is tasked with to investigate, and it implemented all safeguards and rights of its predecessor agreements and the Colombian National Police was designated as the only competent authority to receive information.

The most recently concluded agreements with Albania, Bosnia and Herzegovina, Liechtenstein, Moldova, Montenegro and Serbia were signed over a period from 2013 to 2016, and they all share a common blueprint. They specifically mention the combatting of terrorism as their purpose and establish reciprocal obligations for the protection of personal data. These includes the purpose specification principle that needs to be recognised both in transfer and use of personal data, protection of special categories data, rights of access, correction, deletion for data subjects and renewable retention periods of three years. Like all agreements concluded after 2007, onward transfer of data to third countries and international bodies is possible only with the consent of the transmitting party. Further, the competent authorities to which data may be directly shared by

[231] Agreement on Operational and Strategic Cooperation between Australia and the European Police Office [2007], *supra* note 226

[232] Agreement on Operational and Strategic Co-operation between the Republic of Colombia and the European Police Office, *supra* note 226

Europol or the national contact point are specified, though it is noteworthy that they do not only include police and financial investigation forces, but also national intelligence services as in the case of Albania.

The data protection situation regarding Europol's external relations can therefore be summarised to present a fractured picture. On the one hand, the relationship of the extent to which the EU can impose protection standards on third country partners with the amount of influence the EU has on those parties is indeed observable, most noteworthy in the omission of maximum retention periods in the agreements with the US, Canada and Australia. On the other hand, there has also been a continuous development of the data protection level over the course of time. This might not least be connected to the simultaneous normative development of Europol's regulatory framework and the increased scrutiny through the European Parliament and the CJEU that came with the entry into force of the Treaty of Lisbon. In fact, the high amount of data protection that Europol demands from its partners can apparently also hinder the conclusion of new operational agreements or the upgrading of existing strategic ones if the third country partner shows itself reluctant to implement EU standards, which was emphasised by the failure of the negotiations about an operational agreement with Turkey.[233] Europol also seems to strive for more consistency regarding its external agreements, as the last six accords were adopted under a common blueprint. Furthermore, the continuous development of the agreement's features mirror developments in the EU's general regulatory development concerning data protection, such as the General Data Protection Regulation or the Directive on the protection of natural persons with regard to the processing of personal data for law enforcement purposes. Consistent with the latter, for instance, is the increasing number of regulatory safeguards for determining the source of information. While this increased level of protection is certainly a positive development, some problems nevertheless remain. The standards of the US- and, to a lesser extent, the Canada-Agreement can be regarded as significantly lower than the EU's internal protection standard and a review their transfer rules seems appropriate after 15, respectively 12 years since their conclusion. Such a review would also test to what extent the increased scrutiny regarding Europol would influence the standard of protection in an agreement with partners where the power asymmetry is equal or even tilted towards the third country – which might just as well be a reason for both sides to hold on to the current status quo of their relationship.

[233] E. Ilbiz, C. Kaunert, and D. Anagnostakis, *supra* note 222

6. CONCLUSION

This study provided an analysis of the level of protection the European Union offers regarding the protection of the fundamental rights of privacy and data protection and to what extent these standards are respected in the regulatory frameworks and intelligence exchange actions of the most relevant counter terrorism actors and agreements. Prior to the concluding answer of the initial research question, some remarks about the limitations of this study need to be made. First, it should be noted that while the issue of EU counter terrorism intelligence exchange was addressed from a holistic perspective, the scope of this study was limited and further research is necessary to provide a fully complete assessment of the respective regulatory situation. For instance, a closer analysis of the normative frameworks of databases like the Schengen Information System might have provided additional insights, as would have an analysis of intelligence exchanges that the actors described in this study conduct with other Union bodies that are less directly, but nevertheless relevantly linked to counter terrorism, including for example Frontex and Eurojust. Nevertheless, the research provides for a comprehensive assessment of the research question.

It can be concluded that the extent to which the existing EU regulatory framework on the sharing of intelligence information for countering terrorism respects the rights of individuals is not universal for the entire European Union legal order, but varies along the distinct and incremental paths of European integration. This is most notably observable in the direct comparison of the regulatory framework for non-military actors operating in the AFSJ with the those who are placed in the security and defence dimension of the CFSP. In the former, the increased scrutiny of the European Parliament and the full judicial oversight of the CJEU that followed the entry into force of the Lisbon Treaty have led to a comprehensive data protection framework in which the privacy of personal data is ensured through a wide array of normative safeguards, including amongst others the obligation for fair and lawful processing, source verification, the protection of special categories of data and tight rules for the exchange of data with third countries. This applies both to the regulatory framework of Europol and to the establishment of common rules for the collection and processing of personal data by law enforcement agencies, which rectified the legal protection gap that in the past potentially allowed for the lawful exchange of unlawfully collected information. Additionally, the oversight by independent authorities and the level of protection in Europol's external agreements has steadily increased. Nevertheless, this study also showed that important questions remain regarding the extension of access to databases that originally do not serve a criminal investigation purpose, the inconsistencies of the level of fundamental rights protection in external Europol agreements and

the potential incompliance of bulk data transfers carried out through the TFTP and PNR agreements with the CJEU's requirements for the legality of data retention. While these issues are joint responsibilities of the European Parliament, the Commission and the Council, the parliament can be distinguished as the most important actor for public scrutiny regarding data protection in counter terrorism proceedings. The challenge raised by interoperability should be addressed through a public and parliamentary debate that considers its societal implications, especially regarding vulnerable populations like asylum seekers. The strengthened parliamentary oversight regarding Europol might further have positive effects on the adherence of the institution to its data protection provisions and the ensuring of such provisions in external agreements. Regarding the bulk data transfer agreements, a judicial decision by the CJEU would ultimately be necessary to determine if, to what extent and under which safeguards bulk data may be transferred to third states. Considering the conducted analysis of the technical features of the agreements and the relevant case law, it is argued here that the compliance of the agreements with the CJEU's specifications for the legality of data retention is unlikely.

Despite the described shortcomings and suggestions for improvements, the overall level of protection in the non-military dimension of EU counter terrorism intelligence exchange can be considered to find an adequate balance between the rights of the individual and the operational necessities of countering terrorism.

On the other side, the intergovernmental logic of the institutional counter terrorism intelligence capacity building in the CFSP seems to have prevented a similar amount of transparency and regulatory sophistication for actors operating in the CFSP realm. The study found a large regulatory gap concerning the normative frameworks of INTCEN and INTDIV, which were found to be inadequate for their information exchange actions. This might be explained by the reluctance of national governments and their intelligence services to engage in operational integration and the resulting secrecy with which INTCEN cloaked its activities to foster a higher level of trust. Substantial efforts should be taken to rectify these normative inconsistencies, measures like a task specification and an internal oversight body being examples for how regulatory coherence and individual rights could be more adequately ensured without hampering the intelligence analysts work. Depending on the willingness of the Member States, INTCEN could be given an individual regulatory framework, associated with, but outside of the institutional structure of the EEAS. This would address the problem of an EEAS institution tasked with internal security monitoring, which sits uncomfortably with the provisions of the TEU. It could further clarify the extent to which personal data is exchanged and establish safeguards for such exchanges. As the reluctance of Member States concerning intelligence

capacity integration makes such a codification unlikely, the latter could alternatively be implemented by an amending decision of the High Representative to the existing decision on the rules regarding data protection, which could specify specific rules for counter terrorism intelligence exchanges conducted by INTCEN and INTDIV.

Regarding external agreements and military missions with counter-terrorism information exchange clauses, the extent to which personal data protection is codified apparently correlates with the likelihood that such data might be shared by the EU. This implies a low threat of fundamental rights infringements, however further research on nature and scope of the data that is transferred based on the individual agreements' information exchange provisions is necessary to effectively validate this assessment. The same applies to the CFSP agreements on the exchange of classified information. A solution could be delivered by the Council through an updated regulatory framework for the exchange of classified information, which could either specify that personal data may not be transmitted through respective agreements or lay down specific rules for personal data transfers that are consistent with Directive 2016/680.

In the future, the EU should hold on to the human rights and data protection standards it has committed itself to in its Charter on fundamental rights, and continuously build towards more consistency both in its counter terrorist intelligence exchanges and the respective legal safeguards for the rights of individuals. The development of operational intelligence exchange will need to be coevolutionary with the level of individual protection, which would in principle ultimately require the approximation of intelligence collection standards, parliamentary oversight regarding all EU counter terrorism action and clear rules regarding the access to personal data in EU databases and the exchange of such data between Union bodies tasked with internal security. This underlying logic of integration is obviously far more complex than estimated here and is highly unlikely to produce such results in the near future, but normative consistency, respect for fundamental rights and the rule of law should nevertheless constitute guiding principles for the Union's intelligence based coalescence in the fight against terrorism. Neither one hundred per cent security nor one hundred per cent personal freedom will ever be achieved, but it is in the vital interest of the Union's constitutional values, its citizens and all individuals whose data may be processed by Union institutions that a reasonable balance between these ideals is found.

7. BIBLIOGRAPHY

Academic Literature

A. Amicelle, 'The Eu's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance,' *Liberty and Security in Europe* 2013

J. Argomaniz, 'Post-9/11 Institutionalisation of European Union Counter-Terrorism: Emergence, Acceleration and Inertia,' 18 *European Security* 2009,151-172.

J. Argomaniz, O. Bures, and C. Kaunert, 'A Decade of Eu Counter-Terrorism and Intelligence: A Critical Assessment,' 30 *Intelligence and National Security* 2015,191-206.

D. Bigo et al., 'Mass Surveillance of Personal Data by Eu Member States and Its Compatibility with Eu Law,' 61 *Liberty and Security in Europe* 2013

S. Blockmans et al., 'Eeas 2.0: A Legal Commentary on Council Decision 2010/427/Eu Establishing the Organisation and Functioning of the European External Action Service (February 7, 2013).' *CEPS Paperbacks* 2013

M. D. Boer, 'Counter-Terrorism, Security and Intelligence in the Eu: Governance Challenges for Collection, Exchange and Analysis,' 30 *Intelligence and National Security* 2015,402-419.

J. v. Buuren, 'Secret Truth. The Eu Joint Situation Centre.,' *Amsterdam: Eurowatch* 2009

D. L. Carter and J. G. Carter, 'The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement,' 36 *Criminal Justice and Behavior* 2009,1323-1339.

P. P. Craig and G. De Búrca, *Eu Law: Text, Cases, and Materials* (Oxford: Oxford University Press 2015).

M. a. K. D. Cross, 'A European Transgovernmental Intelligence Network and the Role of Intcen,' 14 *Perspectives on European Politics and Society* 2013,388-402.

P. De Hert and S. Gutwirth, 'Interoperability of Police Databases within the Eu: An Accountable Political Choice?,' 20 *International Review of Law, Computers & Technology* 2006,21-35.

D. Drewer and J. Ellermann, 'May the (Well-Balanced) Force Be with Us! The Launch of the European Counter Terrorism Centre (Ectc),' 32 *Computer Law & Security Review* 2016,195-204.

C. Eckes, 'Common Foreign and Security Policy: The Consequences of the Court's Extended Jurisdiction,' 22 *European Law Journal* 2016,492-518.

C. Hamilton, 'The European Union: Sword or Shield? Comparing Counterterrorism Law in the Eu and the USA after 9/11,' *Theoretical Criminology* 2017,1362480616684195.

E. R. Hertzberger, 'Counter-Terrorism Intelligence Cooperation in the Eu,' *European Foreign and Security Studies Policy Program UNICRI* 2007

H. Hijmans, 'Recent Developments in Data Protection at European Union Level,' 11 *ERA Forum* 2010,219-231.

E. Ilbiz, C. Kaunert, and D. Anagnostakis, 'The Counterterrorism Agreements of Europol with Third Countries: Data Protection and Power Asymmetry,' *Terrorism and Political Violence* 2015,1-18.

D. Keohane, 'The Absent Friend: Eu Foreign Policy and Counter-Terrorism,' 46 *JCMS: Journal of Common Market Studies* 2008,125-146.

O. Lynskey, 'Deconstructing Data Protection: The 'Added-Value of a Right to Data Protection in the Eu Legal Order' ' 63 *International and Comparative Law Quarterly* 2014,569-597.

B. Müller-Wille, 'The Effect of International Terrorism on Eu Intelligence Co-Operation,' 46 *JCMS: Journal of Common Market Studies* 2008,49-73.

B. M. Müller-Wille, 'For Our Eyes Only? Shaping an Intelligence Community within the Eu. ,' 50 *Occasional Paper* 2004

C. Murphy, *Eu Counter-Terrorism Law - Pre-Emption and the Rule of Law* (Oxford: Hart Publishing 2012).

C. Murphy and D. Acosta Arcarazo, *Eu Security and Justice Law : After Lisbon and Stockholm* (Oxford: Hart Publishing 2014).

L. Pech, ''A Union Founded on the Rule of Law': Meaning and Reality of the Rule of Law as a Constitutional Principle of Eu Law,' 6 *European Constitutional Law Review* 2010,359-396.

S. Peers, *Eu Justice and Home Affairs Law* (Oxford: Oxford University Press 2011).

A. Roberts, 'Privacy, Data Retention and Domination: Digital Rights Ireland Ltd V Minister for Communications,' 78 *The Modern Law Review* 2015,535-548.

F. Trauner, 'The Internal-External Security Nexus: More Coherence under Lisbon?,' *EU ISS Occassional Paper* 2011

G. Valkenburg, 'Privacy Versus Security: Problems and Possibilities for the Trade-Off Model,' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds), *Reforming European Data Protection Law*(Springer Netherlands, 2015).

B. Van Vooren and R. A. Wessel, *Eu External Relations Law : Text, Cases and Materials* (Cambridge, United Kingdom: Cambridge University Press 2014).

J. I. Walsh, 'Intelligence-Sharing in the European Union: Institutions Are Not Enough*,' 44 *JCMS: Journal of Common Market Studies* 2006,625-643.

Internet Sources

G. Beck, 'Case Comment: C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom Watson & Others', *Eutopia Law* 2017, available at: https://eutopialaw.com/2017/01/13/case-comment-cases-c-20315-tele2-sverige-ab-v-post-och-telestyrelsen-and-c-69815-secretary-of-state-for-the-home-department-v-tom-watson-and-others/

Commission of the European Communities, 'Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice
and Home Affairs' (2005)

Council of the European Union, 'Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism', available at: http://www.consilium.europa.eu/en/press/press-releases/2015/11/20-jha-conclusions-counter-terrorism/

Council of the European Union, 'Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (June 2007), available at: http://europa.eu/rapid/press-release_PRES-07-157_en.htm

Council of the European Union, 'Report on the implementation of the EU Counter-Terrorism Strategy' (November 2014), available at: http://data.consilium.europa.eu/doc/document/ST-15799-2014-INIT/en/pdf

Emily O'Reilly, 'Decision of the European Ombudsman closing the inquiry into complaint 1148/2013/TN as regards Europol LIBE Committee', European Parliament, Brussels, Thursday 8 Jan 2015, available at: http://statewatch.org/news/2015/feb/ep-omb-speech-europol-15.pdf

EU Law Blog: 'Judgment in PNR cases : Cases C-317/04 and C-318/04', available at: http://eulaw.typepad.com/eulawblog/2006/05/judgment_in_pnr.html

EU global strategy on foreign and security policy, available at: <http://www.eeas.europa.eu/ archives/docs/top_stories/pdf/eugs_review_web.pdf >

European External Action Service, 'EU INTCEN Factsheet' (2015), available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160615factsheetintcen_/sede160615factsheetintcen_en.pdf

European Commission, 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders' (2016), available at: http://statewatch.org/news/2016/sep/eu-com-security-mobility-info-exchange-com-602-final.pdf

European Commission, 'Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' (January 2017), available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_swd_en.pdf

European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice'

(Brussels, 25 November 2014), available at: http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice
Europol, 'Data Processing at Europol – Who, Where and How?', available at: https://www.europol.europa.eu/st/DPO/#/methods_and_means
Europol, 'Europol Analysis Projects', available at: https://www.europol.europa.eu/crime-areas trends/europol-analysis-projects.
Europol, 'New AWF Concept - Guide for MS and Third Parties' (2012), available at: http://www.statewatch.org/news/2013/jan/europol-awf-new-concept.pdf
Europol, 'Q&A: The EU–US TFTP Agreement' (2011), available at: https://www.europol.europa.eu/ publications-documents/qa-eu%E2%80%93us-tftp-agreement-0
Europol, 'Transparency', available at: https://www.europol.europa.eu/about-europol/transparency
O. Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change', *European Law Blog* 2017, available at: https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/
E. Lichtenstein and J. Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror', *The New York Times,* 23 June 2006, available at: http://www.nytimes.com/2006/06/23/washington/23intel.html
E. McKirdy and A. Dewan, 'UK police face questions as third London attacker named', *CNN International Edition,* (London, 6 June 2017), available at: http://edition.cnn.com/2017/06/06/europe/london-terror-attack/index.html
C.D.F. Maesa, '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)', *Eurojus.it* 2016, available at: 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/

Cases

ECJ, Case 294/83 *Les Verts* v. *Parliament* [1986]
ECJ, Case C-317/*04 European Parliament* v *Council* and Case C-317/04 *European Parliament* v *Commission,* [2004]
ECJ, C-524/06, *Huber* v. *Germany* [2008]
ECJ, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014]
ECJ, Joined Cases (C-203/15) and (C-698/15), *Tele2 Sverige AB* v *Post- och telestyrelsen***,** and *Secretary of State for the Home Department* v *Tom Watson, Peter Brice, Geoffrey Lewis, interveners: Open Rights Group, Privacy International, The Law Society of England and Wales* [2016]

Legislation

Agreement between Georgia and the European Union on security procedures for exchanging and protecting classified information, *OJ* [2016] L 300/4, 8.11.2016
Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *OJ* [2010] L 195/5, 27.7.2010
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, *OJ* [2012] L 186/8, 14.7.2014, Art. 16
Agreement between the United States of America and the European Police Office [2001], available at: https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1
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, *OJ* [2012] L 215/5, 11.8.2012
Charter of Fundamental Rights of the European Union, *OJ* [2012] C 326/391, 26.10.2012
Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, *OJ* [2006] L 91/49, 29.3.2006
Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, *OJ* [2012] C 326, 26.10.2012
Co-Operation Agreement between the Government of Canada and the European Police Office [2005], available at: https://www.europol.europa.eu/partners-agreements/operational-agreements
Council Decision of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP OJ [2003] L 16/68, 22.1.2003
Council Decision 2012/312/CFSP of 16 July 2012 on the European Union CSDP mission in Niger (EUCAP Sahel Niger), *OJ* [2012] L 187/48, 17.7.2012
Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union, OJ [2001] L 27/7, 30.1.2001
Council Decision of 23 September 2013 on the security rules for protecting EU classified information, *OJ* [2013] L 274/2, 15.10.2013
Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service, OJ [2010] L 201/30, 3.8.2010
Council Decision of 6 April 2009 establishing the European Police Office (Europol), *OJ* [2009] L 121/37, 15.5.2009
Council Framework Decision of 13 June 2002 on combating terrorism, *OJ* [2002] L 164/5, 22.6.2002
Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ [2008] L 350/60, 30.12.2008
Council Joint Action Plan 2008/124/CFSP of 4 February 2008, on the European Union Rule of Law Mission in Kosovo, EULEX KOSOVO, *OJ* [2008] L 42/92, 16.2.2008
Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection, OJ [2012] C 308/8, 12.10.2012
Directive 2016/680 of the European Parliament and 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, *OJ* [2016] L 119/105, 4.5.2016
Directive 95/46 EC of the European Parliament and 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, OJ [1995] L281/38, 23.11.1995
Euro-Mediterranean Agreement establishing an Association between the European Communities and their Member States, of the one part, and the Arab Republic of Egypt, of the other part, *OJ* [2004] L 304/39, 30.09.2004
Euro-Mediterranean Agreement establishing an Association between the European Community and its Member States, of the one part, and the People's Democratic Republic of Algeria, of the other part, *OJ* [2005] L 265/2, 10.10.2005
Joint communication to the European Parliament and the Council, 'Joint Framework on countering hybrid threats, a European Union response' (April 2016), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Iraq, of the other part, *OJ* [2012] L 204/18, 31.07.2012
Partnership and Cooperation Agreement establishing a partnership between the European Communities and their Member States, of the one part, and the Republic of Tajikistan, of the other part, *OJ* [2009] L 350/1, 29.12.2009
Political Dialogue and Cooperation Agreement between the European Community and its Member States,

of the one part, and the Republics of Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama, 01.05.2014

Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ* [2016] L 135/53, 24.5.2016

Regulation 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ* [2001] L 8/1, 12.1.2001

Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Albania, of the other part, OJ [2009] L107/166, 28.04.2009

Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, *OJ* L 278/16, 18.10.2013

Supplemental Agreement between the Europol Police Office and the United States of America on the Exchange of Personal Data and related Information [2002], available at: https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1