FACULTY OF LAW
Lund University

Wandee Setthapirom

Safeguarding Financial Integrity and Privacy in the EU's Internal Market:

Balancing Anti-Money Laundering Obligations against Fundamental Rights to Privacy

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Eduardo Gill-Pedro

Term: JAEM03

Table of Contents

Summary

The thesis explores the EU's anti-money laundering framework's compatibility with conditions required under privacy rights. It asks the question whether the anti-money laundering framework confers obligations to private entities and other actors not belonging to law enforcement in a way which risks violation to the fundamental rights to privacy and data protection. The thesis elucidates the significance of privacy rights in the EU as underpinned by the principles of privacy in the European Convention of Human Rights. Moreover, the thesis examines the lawful conditions for far-reaching data-processing. It clarifies that the cases of the Court of Justice of the European Union require, among other conditions, clear and precise rules to limit the extent of interference of the right to privacy and, a link to serious crimes, to process personal data in a far-reaching manner. Additionally, the thesis highlights the complementary role of the General Data Protection Regulation in support of privacy rules within the internal market.

It finds that the AML-directives rely on private entities for the detection, monitoring and reporting of all individuals using financial services while including few safeguards to limit the interference with the right to privacy. Instead, the AML-directives direct the responsibility of safeguarding data protection to the Member States, despite providing few incentives for the adequate protection of data privacy while fulfilling the AML-objectives. Furthermore, it is found that there is uncertainty regarding which data-protection framework a financial intelligence unit must be subject to, resulting in discrepancies in data-protection commitments during the request of exchange for information. Consequently, another Member State's financial intelligence unit has access to a vast amount of personal data with little to no restriction. It therefore states that there are multiple risks of violation of the EU Charter as Member States are required to navigate and comply with the conflicting AML-obligations and the robust privacy rights.

Against this background, the thesis concludes that there are risks that Member States violate the principles of necessity and proportionality under Article 52(1) of the EU Charter due to the incoherency of norms. Lastly, the thesis reiterates the commercial roots upon which the internal market is established could lead to an overshadowed fundamental rights protection while prioritising commercial mobility using Article 114 TFEU. Consequently, such legal incoherency could erode the privacy rights established under Articles 7 and 8 of the EU Charter, overshadowing the fundamental right to privacy.

Abbreviations

AML	Anti-Money Laundering
CJEU	Court of Justice of the European Union
EBA	European Banking Authority
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU Charter	EU Charter of Fundamental Rights
FATF	Financial Action Task Force
FinTech	Financial Technology
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
NPPS	New Payment Products and Services
PEP	Politically Exposed Persons
SOCTA	Serious and Organised Crimes Trends Assessment
TESAT	Terrorism Situation and Trend Report
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

1. Introduction

The EU and its removal of barriers to trade has entailed a commercial mobility which incentivises free movement of innovative financial services throughout the internal market. The legal and political commitments have resulted in a cooperation for businesses to thrive, expand their operations, and tap into a vast consumer base.[1] However, the possibilities offered by the internal market are also exploited by criminal and terrorist activities, where businesses of various sectors in the EU are used for money laundering and terrorist financing.[2] The influx of illegal proceeds into the EU's economy harms the international development of the EU's financial sector as the four freedoms of the EU are abused for illicit purposes while enabling criminal and terrorist organisations to expand.[3] Through the exploitation of businesses and bribery of politically exposed persons or persons in sectors such as healthcare, pharmaceuticals, construction, education, the very foundations of the internal market is undermined.[4] This threatens the financial integrity, stability and credibility of the EU.[5] Due to the obscure nature of money laundering and terrorist financing, detection and investigation is difficult.[6]

To tackle these threats, the EU has introduced a comprehensive set of legislative measures aimed at combating money laundering and terrorist financing. The Anti-Money Laundering (AML) Directives are intended to fight two crimes, namely, the concealing of the origin of illicit money (money laundering), and the redistribution or integration of the laundered funds back to use for terrorist activities through investments into businesses, organisations, or the purchase of goods (terrorist financing).[7] These measures rely on private entities and financial intelligence units to monitor, gather and detect risks of money laundering and terrorist financing through analysing personal data of their customers.[8]

However, the obligations to conduct customer due diligence and monitor customers have not come without their share of controversy and implications for the fundamental rights to privacy of individuals. In the pursuit of cracking down on illicit transactions and terrorist financing, private entities and other actors have been entrusted with investigative tasks and obligations. Consequently, the cooperation between private entities and other actors, as laid down in the regulatory structure of the AML-directives, creates a tension between the objective of fighting money laundering and the fundamental rights to data protection and privacy, raising concerns

[1] Catherine Barnard, *The Substantive Law of the EU, The Four freedoms* (6th edition OUP 2019) 16.
[2] Europol, 'Serious and Organised Crime Threat Assessment, a Corrupting Influence: the Infiltration and Undermining of Europe's Economy and Society by Organised Crime (2021) Europol <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021>, Accessed 21 May 2023, 14 and 15. Hereinafter referred to as "SOCTA".
[3] ibid, 26.
[4] ibid, 15 and 26.
[5] ibid.
[6] ibid, 14-15.
[7] Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May [2015] on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141. (Hereinafter '4th AML-directive') Recital 4 and Article 1(2)-(3).
[8] Article 11(e)-(f) 4th AML-directive.

about the potential erosion of the robust privacy norms that are rooted in the EU's Charter of Fundamental Rights.[9]

1.2 Purpose and research question

The aim of the thesis is to explore whether the AML-directives and its reliance on private entities and financial institutions to gather personal data risk violating the EU's privacy rights. Moreover, the AML-obligations are scrutinised in the light of EU privacy rights and examines the limitations that the GDPR imposes on personal data gathering under the AML-framework. Overall, the thesis aims to elucidate the contingency between AML obligations and EU privacy rights. The following research questions will be answered to fulfil the aims of this thesis:

1. Do the AML-directives require private entities and financial intelligence units to scrutinise individuals in a way which risks violation of EU privacy rights?

2. What are the conflicts between the AML-obligations and EU privacy rights?

1.3 Method and material

To fulfil the aim of the thesis and explore the gathering of personal data under the AML-directives, the EU legal method is applied. This methodology is suitable to answer the research questions as legal sources of the EU and must be examined. The EU legal method is suitable for the analysis of the norms and AML-Directives and the EU level, while also considering the potential risks which may emerge upon implementation at the Member State level.[10] The EU legal method is suitable for the understanding of the hierarchy of legislations when navigating primary legislation and secondary legislation.[11] In applying the EU legal method, the foundation of the EU is laid out, describing the creation of the internal market and its principles facilitating intra-union trade, and second, the development of the EU Charter. The EU legal method will also serve to include cases of the CJEU and the ECtHR, which must be examined to explain the foundations of the internal market and the EU Charter. This is necessary to achieve the purpose of the thesis where it requires an analysis of privacy norms within the EU and its interaction with EU bodies, Member States, and private entities in the internal market.

The cases of the ECtHR and the CJEU are included to illustrate the regulatory environment of privacy protection within the EU, which is important to form a critical standpoint in the analysis of the AML-directives' compatibility with the fundamental rights. The contextualisation of fundamental rights principles concerning privacy is also found in the adoption of the GDPR, which further demonstrates commitments undertaken by the EU. Lastly, to highlight the

[9] The European Data Protection Board, 'Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing' [2020] <https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_en> Accessed 25 May 2023.
[10] Jane Reichel, 'EU-rättslig metod' in Nääv, Maria & Zamboni, Mauro (red.), Juridisk metodlära, (2nd Studentlitteratur AB, Lund, 2018) 109–111.
[11] ibid, 109.

conflicts between the AML-obligations and EU privacy rights, an analysis is made through comparing the legal instruments and criticising the incoherencies between the frameworks.

Moreover, to understand the EU's AML efforts, the method provides for the inclusion of soft law instruments which are guidelines, handbooks, communications, white papers, and other official publications relating to the cooperation against money laundering and terrorist financing within the EU.[12] The EU legal method also enables the inclusion of instruments published by expert bodies (such as the FATF) who are tasked to publish guidelines and recommendations that directly impact the AML-directives.[13] More materials from expert bodies include letters and a statement from the EDPB and the EDPS for their critique about the compatibility of the AML-measures with the EU privacy rights. Additionally, guidelines of the EBA are included for their detailed clarification of measures which must be carried out by private entities, specifically where it involves the gathering of personal information. Furthermore, reports from Europol are examined to understand the rationale behind the measures reflected in the AML-directives, particularly for their assessment of serious and organised crimes and the situation of financial crimes in the EU. Secondary sources such as literature, journal articles and reports are included to achieve the purpose of the thesis where it is necessary to analyse the field of AML and privacy protection in the EU. The secondary sources enable in-depth perspective of respective fields (AML and privacy rights) as the authors provide expertise on the matters. Lastly, electronic sources are included for their additional information concerning specific concepts not explained in the secondary sources.

1.4 Delimitations

The thesis focuses on the practical implications to privacy rights in the Member State's implementation of AML-obligations applied by private entities and financial intelligence units. Although the thesis mentions the broadening of obliged entities to several sectors outside of financial service providers, it excludes the in-depth examination of such sectors, including virtual currencies which are commonly exploited by terrorist actors for their anonymity as such would go beyond the scope of the thesis. Furthermore, the thesis limits itself to the private entities' cooperation with each other and FIUs, which is directly required by the AML-directives for information-sharing on a regular basis. This means that the cooperation between private entities and law enforcement agencies will not be analysed due to the differing coercive mechanisms afforded by criminal law to law enforcement agencies. Although there is international cooperation in the AML-frameworks, the thesis limits itself to matters directly relating to the EU's efforts and the measures taken to tackle money laundering and terrorist financing within the internal market. As such, third countries and international frameworks outside of what is directly related to EU's internal AML-measures are excluded. Concerning the prohibition of terrorist financing, the thesis will not include the EU's efforts in counter terrorism as it only focuses on the abuse of the EU's *financial system* and does not intend to explore terrorist use of the laundered funds. Although the thesis mentions 'mutual trust', it does not examine the area of freedom, security and justice (AFSJ) of the EU. It only focuses

[12] ibid, 127.
[13] ibid, 125; Recital 4, 4th AML-directive.

on the difficulties for the Member States to refuse information-exchange, thus limiting itself within the scope of the research questions.

1.5 Outline

The 1st chapter introduces the topic of money laundering and terrorist financing in the internal market. It lays down the purpose and research question of the thesis. It also explains the delimitations, method and materials used to answer the research questions.

The 2nd chapter explains the creation of the internal market and its significance for commercial mobility and innovations across the EU. It elaborates that the legal instruments such as the Treaty of the European Union and the Treaty of the Functioning of the European Union enables intra-union trade, for example, through establishing the four freedoms. It highlights how case law from the CJEU facilitates cross border commercial activities which are vital for the functioning of the internal market. It then explains the legal mechanisms used by the EU to introduce harmonisation and thereby remove legal and technical barriers to trade, which further helps businesses to operate. The chapter emphasises the role of private entities as the backbone of the European economy where free movement of goods, workers, establishments, services, and capital must be safeguarded against barriers threatening its functioning. Furthermore, the EU's fundamental rights regime is explained, starting with its development, creation, and significance. It delineates the scope of the fundamental rights and explains the inapplicability of national fundamental rights standards where it undermines the *unity, primacy and efficiency* and is incompatible with the EU Charter. At the end of the chapter, EU fundamental rights is contextualised by describing its impact on the internal market and the private entities operating therein.

The 3rd chapter describes the right to private life and personal data in the EU. Its importance is highlighted through its historical roots where it is established for the protection of fundamental rights and freedoms of persons in Articles 7 and 8 of the EU Charter. Furthermore, the case law of the CJEU is examined to describe the normative approach of the EU: the economic and the fundamental right combined. The key takeaways of those cases are highlighted where the right to privacy and the right to data protection are viewed as independent rights which are interconnected. The chapter emphasises conditions for different situations in which far-reaching measures can be applied lawfully. At the end of the chapter, an explanation of the General Data Protection Regulation and a brief explanation of the Law Enforcement Directive is included. Both are important data protection frameworks which emanate the principles of Articles 7 and 8 of the EU Charter.

The 4th chapter focuses on the criminal exploitation of the mobility and freedoms guaranteed by the internal market. Since the internal market is the cornerstone of the EU and the functioning of it is vital for businesses and consumers alike, the abuse of businesses operating therein threatens the financial integrity, credibility, and stability of the EU. The chapter exemplifies the *modus operandi* of criminal organisations and terrorist groups where financial technology services are used to launder money. It also describes how the intertwining of licit

and illicit funds harms the different sectors operating in the internal market through bribery of politicians or persons in important sectors (pharmaceuticals, construction, education). Overall, this chapter illustrates the different actors partaking in the intentional and unintentional funding of terrorism while highlighting the obscure nature of money laundering.

The legal efforts made to tackle money laundering and terrorist financing is elucidated in the 5th chapter. It provides an overview of the plethora of actors tasked to cooperate and develop guidelines in the field of anti-money laundering countermeasures. Moreover, a brief explanation is given concerning the harmonisation of the previously diverging approaches of the Member States. The chapter then explains the contemporary AML-directives which are applied by private entities. Among other obligations, the chapter describes the duties of the private entities and the financial intelligence units to conduct risk assessments, customer due diligence-measures, monitor, report, and exchange information about individuals.

In the 6th chapter, the AML-obligations of private entities and financial intelligence units are scrutinised in the light of the right to private life and personal data. It explains how the robust regime of privacy protection risks irreconcilability with the far-reaching obligations when the directives lack provisions which limits the interference of privacy and leaves the discretion of protection to the Member States. Specifically, the 6th chapter addresses the risks of violation of the right to private life as private entities and financial intelligence units are carrying out their obligations without explicit restrictions laid out. The chapter details the previously laid out principles of privacy protection and contextualises the conditions for far-reaching processing of personal data against the application of AML-obligations. Finally, the powers of financial intelligence units are criticised for lacking explicit restrictions despite their access to a vast amount of information on individuals.

The 7th chapter concludes the thesis by presenting the answer to the research questions. It concludes that the AML-obligations confer obligations in a manner which creates multiple risks of violating the right to private life with the right to personal data when implementing the EU directives. It highlights the robustness of the privacy-frameworks and shows the difficult reconciliation between requirements of ‘clear and precise rules’ to limit the interference of the right to private life and the obligations to analyse and continuously monitor individuals. Lastly, the chapter reiterates the commercial nature of the EU as the guardian of the internal market. Closing remarks are then made to criticise the commercial approach adopted to tackle crimes since it potentially weakens the EU’s credibility in handling fundamental rights.

2. The Internal Market as the Cornerstone of the European Union

The internal market can be viewed as one of the EU's greatest achievements.[14] From the start of the formation of what would become the European Union (EU), ambitious plans concerning the establishment of a single economy were laid out in the 1950's.[15] The aim was to facilitate trade between Member States without hindrances such as customs duties and charges with equivalent effect.[16] For these reasons, the EU has always been an economic entity with a strong focus on the formation of 'a system ensuring that competition in the common market is not distorted', a system also referred to as 'economic integration'.[17] Later in its development, the Treaty of Rome was adopted and the legal foundations for the internal market were established. The provisions of the Treaty of Rome enabled freedom of movement for factors of production such as workers, goods, establishment, services, and capital.[18] In contemporary times, the Treaty of Rome was amended and renamed Treaty on the Functioning of the European Union (TFEU) and the Treaty of European Union (TEU) was introduced. The TEU brought important changes which further strengthened the internal market through the inclusion of provisions necessary for the facilitation of free movement of goods, services, capital and persons, and EU citizenship among others.[19] Importantly, Article 3 TEU encapsulates the link between the internal market and other, wider objectives of the EU. Since the EU is entrusted with the pursuit of those objectives, Article 3(3) TEU explicitly stipulates that it shall establish an internal market. Those objectives alongside its four freedoms exist to contribute to the implementation of the economic integration, which is viewed as the *raison d'être* of the EU itself.[20]

2.1 Removal of Trade Barriers to Facilitate Intra-union Trade

To prevent Member States from introducing hindrances to the cross-border trade, the EU may *prohibit* national rules which are either discriminatory or because they hinder market access, a measure referred to as *negative integration*.[21] Another essential component of the internal market occurs through reliance on Articles 114 and 115 TFEU, where a *positive integration* can be applied. *Positive integration* means harmonisation of diverse rules across the Member State. Harmonisation is an essential tool of free trade within the single market, as it unifies diverse provisions among its Member States, reducing unpredictable standards and

[14] Commission, 'Upgrading the Single Market: more opportunities for people and business' (Communication) COM (2015) 550 final.
[15] Robert Schütze, *European Union Law* (2nd edition, Cambridge University Press 2018) 774.
[16] Paul Craig, 'The Evolution of the Single Market' in Catherine Barnard, and Joane Scott (eds), *The Law of the Single European Market: Unpacking the premises*, (Bloomsbury Publishing Plc 2002) 3.
[17] ibid, 1-2; Ex Article 3(f) Treaty of Rome (EEC).
[18] Michelle Egan, 'Single Market' in Erik Jones (ed.) et al, *The Oxford Handbook of the European Union* (OUP 2012) 408.
[19] Articles 56-60 TFEU enshrines the four freedoms.
[20] Opinion 2/13 pursuant to Article 218(11) TFEU, ECLI:EU:C:2014:2454, European Union: Court of Justice of the European Union, 18 December 2014, para 172.
[21] Paul Craig and Gráinne de Búrca, *EU Law, Text, Cases, and Materials* (6th edition OUP 2015) 608.

regulations.[22] Both *negative integration* as well as *positive integration*-measures are aimed at reducing barriers to cross-border trade within the internal market.

Furthermore, EU law has gone further than merely prohibiting tariff barriers by prohibiting non-tariff barriers and measures having equivalent effect (Articles 34-5 TFEU).[23] It also prohibits anti-competitive behaviours (Articles 101 and 102 TFEU) and state aids (Article 107 TFEU).[24] In turn, intra-union trade is facilitated and thus believed to increase the competitiveness of the European industry.[25] Additionally, there are multiple legal bases permitting the EU to regulate the internal market under, such as Article 43 TFEU (agriculture), Article 73 TFEU (industrial policy) and Article 192 TFEU (environment). As the internal market evolved over time, case *Titanium Dioxide* elucidates how the Court of Justice of the European Union (CJEU) favours Article 114 TFEU over the specific provision for regulating the environment (Article 192 TFEU).[26] In *Titanium Dioxide*, the CJEU argued that diverse environmental and health regulations across the Member States were a burden on *undertakings* operating on the market, and that competition could be distorted in the absence of harmonisation under 114(1) TFEU.[27]

Another integral part of the EU's strategy for the internal market is the mutual recognition principle established in case *Cassis de Dijon.*[28] The mutual recognition principle is a normative dimension which establishes that products which are manufactured and sold in one Member State must be able to be lawfully sold in any other Member State.[29] This principle is important for the mutual respect between Member States and restrain Member States from imposing their own trade-restricting rules. Nevertheless, *Cassis de Dijon* also lays down rules in which a Member State can impose restrictions to trade, such as when mandatory requirements are successfully invoked. Mandatory requirements include the protection of public health, fairness of commercial transactions and the defence of the consumer.[30] In short, the effect of *Cassis de Dijon* is negative and deregulatory, as it removes trade barriers which could not be justified by mandatory requirements.[31]

2.2 The Role of Private Entities in the Functioning of the Internal Market

The introduction of Article 114 TFEU marks the significance of the internal market as a lawmaking project facilitating intra-union trade between enterprises.[32] Considering the efforts taken to create a favourable legal climate for undertakings, the preferred application of Article

[22] Catherine Barnard (n 1) 560-561 and 573.
[23] Case C-8/74 *Procureur du Roi v Benoît and Gustave Dassonville* [1974] ECLI:EU:C:1974:82.
[24] Catherine Barnard (n 1) 14.
[25] Jacques Pelkmans, 'The New Approach to Technical Harmonization and Standardization' (1987) 25 JCMS 249, 256 and 260.
[26] Catherine Barnard (n 1) 573; Case C-300/89 *Titanium Dioxide* [1991] EXR I-2867, para 20.
[27] ibid, 573.
[28] Paul Craig and Gráinne de Búrca (n 21) 622.
[29] ibid, 610-611.
[30] Paul Craig (n 16) 7.
[31] ibid.
[32] Catherine Barnard (n 1) 16.

114 TFEU also demonstrates the important role of private undertakings and their relation to the internal market.[33] This notion is further strengthened by commitments set out by the EU Commission to strengthen the industrial base of the internal market. In a Communication,[34] the EU Commission described private undertakings, consumers, investors and businesses as crucial actors in the economic ecosystem in the Single Market.[35] Moreover, small to medium enterprises are held as the 'backbone of the European economy' as the EU Commission urges the European Parliament and the Council to support the commitments to improve cross-border trade 'in the interests of citizens and businesses across Europe'.[36] Considering the establishment of a complex legal regime which facilitates free movements of goods, workers, establishment, services and capital, this further highlights the relation between the internal market and the private undertakings functioning as pillars of the internal market. Considering the strong efforts to create a single economy made from the start of the EU to its recent years, it is evident that the internal market is the political and legal project which would become the cornerstone of the EU.[37]

2.3 The EU Charter in the Internal Market

Human rights laws are given a fundamental value in European society where their role serves as binding moral and legal obligations which can hold states accountable for their actions, or to create responsibilities which must be ensured.[38] Fundamental rights can only be limited if necessary, provided by law, with respect given to the essence of those rights and subject to the principle of proportionality.[39] They must also genuinely meet objectives of interests recognised by the EU.[40] The main instruments enshrining fundamental rights within the EU are the General Principles of the EU, the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (hereinafter the EU Charter).[41] Before the early development of fundamental rights within the EU, there was no written bill of fundamental rights. In the absence of a written EU fundamental rights, the CJEU expressed in case *Internationale Handelsgesellschaft* that:

> 'In fact, respect for fundamental rights forms an integral part of the general principles of law protected by the Court of Justice. The protection of such rights, whilst inspired by the

[33] ibid, 16-17 and 19-20.
[34] COM (2015) 550 final (n 14).
[35] ibid, 3.
[36] Ibid, 20.
[37] Paul Craig and Gráinne de Búrca (n 21) 607.
[38] ibid, 420 and 427; Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (1st edition, Cambridge University Press 2012) 498. The European Court of Human Rights is perceived to have acquired an expertise and a moral stature. Similarly, the ECHR and the EU Charter which are given equivalent value by virtue of Article 6 TEU, must be viewed as those instruments from which legal and moral obligations flow from within the EU.
[39] Article 52(1) of the EU Charter; Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (1st edition, Cambridge University Press 2012) 498 (2016). According to Aharon Barak, fundamental rights are viewed as inhibiting an untouchable core, in line with the *absolute theory*.
[40] Case C-601/15 *J. N. v Staatssecretaris van Veiligheid en Justitie* [2016] EU:C2016:84, para 50.
[41] Robert Schütze (n 15) 446.

> constitutional traditions common to the Member States, must be ensured within the framework of the structure and objectives of the Union.'[42]

Hence, the CJEU discovered 'General Principles' of EU law in which fundamental rights form an integral part of. It was inspired by the constitutional traditions common to the Member States.[43] The absence of a written instrument of fundamental rights was also solved in case *Internationale Handelsgesellschaft* where the CJEU dismissed the applicability of national fundamental rights to EU law.[44] This notion of primacy of EU General Principles is confirmed in several cases where Member States challenged EU acts on the grounds that it infringed national fundamental rights.[45] Similarly, case *Stork* demonstrated the primacy of EU law as the CJEU confirmed that EU laws 'will be applied without regard for their validity under national law'.[46]

In the EU's search for fundamental rights which are binding and above the Member States' constitutional laws, the ECHR was already an international human rights-instrument agreed upon by EU Member States. The ECHR therefore laid the first ground for the creation of the EU Charter.[47] Despite the inspiration drawn from the ECHR, there is a complex relationship between the CJEU and the European Court of Human Rights (ECtHR), resulting in a non-binding status of the ECHR within EU law.[48] Regardless of the tensions between the courts, fundamental rights recognised by the ECHR forms part of the General principles of EU law. As such, certain cases and provisions of the ECHR have been referred to by EU bodies in EU acts and cases.[49] Today, EU fundamental rights are also reflected in Article 6 TEU, where the legal value of the EU Charter is held to be the same as the Treaties.[50] In addition, Article 52(3) of the EU Charter stipulates that:

[42] Case 11-70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970] ECLI:EU:C:1970:114, paras 3-4.
[43] ibid.
[44] ibid, paras 2-3.
[45] Case no 1-58 *Friedrich Stork & Cie v High Authority of the European Coal and Steel Community* [1959] ECLI:EU:C:1959:4.
[46] ibid, para 26. Similarly, EU primacy is upheld in case *Case 4-73 J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities* [1974] ECLI:EU:C:1974:51.
[47] Robert Schütze (n 15) 447-448.
[48] Xavier Groussot, Tobias Lock and Laurent Pech, 'EU Accession to the European Convention on Human rights: a Legal Assessment of the Draft Accession Agreement of 14th October 2011' (2011) Fondation Robert Schuman, European Issues N°218; Opinion 2/94 pursuant to Article 228 of the EC Treaty, Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms, ECLI:EU:C:1996:140, 28 March 1996.
[49] Article 6(3) TEU; The CJEU interprets cases of the ECtHR in an autonomous way where differences in approach to the same matter may surface. Case *Åkerberg Fransson* showcases this phenomenon in the interpretation of *ne bis in idem* as stipulated in both Article 4 of the ECHR and in Article 50 of the EU Charter.
[50] Article 6(1) TEU.

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.[51]

2.4 EU Fundamental Rights and its Scope of Application

Article 51 of the EU Charter sets out the scope of application of the EU fundamental rights where it requires that the institutions and bodies of the EU respect the obligations therein. At the same time, the principle of sincere cooperation in Article 4(3) TEU stipulates that Member States are obliged to take appropriate measures to ensure that obligations arising out of EU acts are fulfilled.[52] Therefore, Member States must also observe EU fundamental rights in certain situations, such as when implementing EU law.[53] The EU Charter therefore has a vertical application, as seen in case *Wachauf* where it was laid out that the fundamental rights must be upheld when Member States are acting 'in the scope of EU law'.[54] Additionally, case *Bostock* confirms that the requirements flowing from the fundamental rights are binding upon Member States when *implementing* EU law.[55] This rule also applies to central authorities, regional or local bodies and public organisations when implementing EU law.[56] Another situation in which fundamental rights of the EU apply is when Member States derogate from EU fundamental rights on the grounds listed in Article 52(1) of the EU Charter.[57]

2.4.1 The applicability of national fundamental rights to EU law

When it comes to Member States' possibility to apply national human rights standards that provide a *stronger* protection of human rights, Article 53 of the EU Charter leaves a certain discretion for national courts to apply national laws, provided that it is subject to the principles of *primacy*, *unity*, and *effectiveness* of EU law, and does not undermine the fundamental rights.[58]

In case *Melloni*, the Spanish constitutional law allows an opportunity for retrial in cases where a conviction was tried *in absentia*. This fundamental right did not exist in Italy, where the defendant was waiting to be extradited to. Therefore, the Spanish Constitutional Court made a preliminary reference to the CJEU concerning the possibility to apply Spanish fundamental rights under Article 53 of the EU Charter and thus refuse to execute a European Arrest Warrant.

---

[51] Article 52(3) EU Charter. It is important to highlight that the EU is not bound by the cases of the ECtHR despite its expertise in interpreting human rights law. Due to their expertise however, the CJEU may use its case law as guidance for interpretation. More about this complicated relationship is covered in Xavier Groussot et al (n 45).
[52] Opinion 2/13 pursuant to Article 218(11) TFEU, *Draft international agreement, Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Compatibility of the draft agreement with the EU and FEU Treaties*, ECLI:EU:C:2014:2454, para 173.
[53] Robert Schütze (n 15) 476.
[54] Case 5/88 *Wachauf* [1989] ECR 2609, para 19; Case C-260/89 *ERT* [1991] ECLI:EU:C:1991:254; Case C-309/96 *Annibaldi* [1997] ECLI:EU:C:1997:631.
[55] Case C-2/92 *Bostock* [1994] ECLI:EU:C:1994:116, para 16.
[56] European Parliament, Council of the European Union, European Commission, 'Explanations relating to the Charter of Fundamental Rights' [2007] O.J C 303. See 'Explanation on Article 51'.
[57] Case C112/00 *Schmidberger v Austria* [2003] ECLI:EU:C:2003:333.
[58] Paul Craig and Gráinne de Búrca (n 21) 400; Opinion 2/13 (n 52) paras 187-188; Case C-399/11 *Melloni* [2013] ECLI:EU:C:2013:107, para 80.

The CJEU ruled that such an interpretation of Article 53 of the EU Charter by the Spanish court would undermine the primacy of EU law. Case *Melloni* thus showed that Member States cannot disapply EU law as they are 'fully in compliance with the Charter where they infringe the fundamental rights guaranteed by that State's constitution.'[59] The CJEU elaborates that:

> (…) allowing a Member State to avail itself of Article 53 of the Charter to make the surrender of a person convicted *in absentia* conditional upon the conviction being open to review in the issuing Member State, a possibility not provided for under Framework Decision 2009/299, in order to avoid an adverse effect on the right to a fair trial and the rights of the defence guaranteed by the constitution of the executing Member State, by casting doubt on the uniformity of the standard of protection of fundamental rights (…) would undermine the principles of mutual trust and recognition which that decision purports to uphold and would, therefore, compromise the efficacy of that framework decision.[60]

In short, allowing Spain to apply its national constitutional rights would, as stated by Gráinne de Búrca, 'cast doubt on the uniformity of the standard of protection of fundamental rights defined in that framework decision' while also undermining mutual trust and recognition between Member States'.[61] Therefore, if a Member State wants to rely on Article 53 to apply its own national fundamental rights standards, the CJEU provided two conditions allowing such. Those conditions are namely: first, the protection provided by the EU Charter is not compromised, and second, that the primacy, unity, and effectiveness of EU law is not undermined.[62] In this case, Spanish constitutional rights were deemed inapplicable.

In another situation, case *TSN* highlights a situation where a national law was applied to provide a more favourable protection of workers health than required by EU law. Directive 2003/88 harmonises workers' holidays where Article 7 of Directive 2003/88 stipulates that workers are entitled to 4 weeks of holiday. Article 15 of Directive 2003/88 provides that Member States may introduce a more *favourable* protection of safety and health of workers. Article 15 also permits the application of collective agreements which provide more favourable conditions to workers. Additionally, the right to paid leave is guaranteed in Article 31(2) of the EU Charter. As the employers and the workers disagreed on the matter, a case was brought to the Finnish labour court which made a preliminary ruling. The national court asked whether a stronger national protection of annual leave may be applied, even when it exceeds the minimum period provided in Directive 2003/88. The CJEU provided that Directive 2003/88 does not prevent Member States from applying a stronger protection of safety and health of workers.[63] When it comes to whether Article 31(2) of the EU Charter is applicable when a stronger national law is applied as permitted in Article 15 of Directive 2003/88, the CJEU provided that the Member State would, with such application of national law, be acting outside the scope of EU law.

[59] *Melloni* (n 58) paras 56–58.
[60] ibid, para 63.
[61] Paul Craig and Gráinne de Búrca (n 21) 400.
[62] *Melloni* (n 58) para 60.
[63] C-609/17 – *TSN* [2019] ECLI:EU:C:2019:981, paras 33 and 40.

Article 31(2) of the EU Charter is therefore inapplicable when the Member State acts outside of EU law.[64]

In short, Article 15 of Directive 2003/88 provides a possibility for the Member State to apply more *favourable* provisions *outside* the scope of the Directive.[65] Therefore, art 31(2) of the EU Charter is not applicable where more favourable national provision is applied, as it falls outside of EU law and thus outside the scope of Article 51(1) of the EU Charter. The national rights do not affect the minimum protection of Directive 2003/88 and does not interfere with any other rules, such as the conditions of *primacy, unity,* and *effectiveness* of EU law. The national rule could thus be applied without clashing with EU law, as it was regarded to fall outside the scope of it.[66]

2.5 Horizontal Application of the EU Charter: Direct and Indirect Obligations for Private Entities

As previously stated, Member States must observe fundamental rights of the EU when implementing EU acts.[67] This means that Member States are bound by the plethora of rights granted by the EU Charter and must therefore ensure that the rules are upheld without introducing their own conditions.[68] This is referred to as *vertical application* of EU fundamental rights as seen in case *Wachauf*, as opposed to the *horizontal application* where private entities are involved. Interestingly, neither the EU Charter nor the ECHR makes a reference to private entities or individuals. However, the CJEU has declared that EU provisions addressed to Member States could in fact impose obligations on individuals, such as in the cases *Defrenne v Sabena* and *Angonese.*[69] Additionally, cases *Mangold* and *Kücükdevici* demonstrate the applicability of explicitly-mentioned General principles in situations where private entities are involved.[70] Therefore, even if the direct imposition of fundamental rights upon private entities may be rare, it is evident that the internal market is affected by the role of fundamental rights.

When it comes to the broader connection between EU fundamental rights and the internal market, EU Directives and EU Regulations may also embody elements and principles derived from fundamental rights.[71] Considering the fact that there are private entities operating within the internal market, which is governed by the rights guaranteed by the EU Charter and ECHR,

---

[64] ibid, paras 52-53.
[65] European Employment Lawyers Association, 'ECJ 19 November 2019, joined cases C-609/17 and C-610/17 (TSN), Paid leave' <https://eela.eelc-updates.com/summary/eelc-2019-317545> Accessed 18 March 2023.
[66] *Melloni* (n 58) para 60; Opinion 2/13 (n 52) paras 188–189.
[67] Paul Craig and Gráinne de Búrca (n 21) 410-411.
[68] *Melloni* (n 58) paras 56-63; Case C-617/10 *Åklagaren v Hans Åkerberg Fransson* [2013] ECLI:EU:C:2013:105, paras 45-46.
[69] Paul Craig and Gráinne de Búrca (n 25) 419; Case 43-75 *Defrenne* [1976] ECLI identifier: ECLI:EU:C:1976:56 paras 31 and 39; C-281/93 Angonese v Cassa di Risparmio di Bologna [2000] ECR I-4134 paras 44-45.
[70] Case C-144/04 *Mangold* [2005] ECLI:EU:C:2005:709, paras 75-77;Case C-555/07 *Kücükdeveci* [2010] ECLI:EU:C:2010:21, paras 50-51.
[71] One example of such would be the General Data Protection Regulation. It directly concerns the right to privacy which is guaranteed in Article 8 ECHR and 7 and 8 of the EU Charter.

their impact on businesses is evident. Examples of frameworks mentioning EU fundamental rights which affect private entities include the Biotechnology Directive, the Audiovisual Media Services Directive, and the Regulation on compensation of passengers for air travel delays.[72] Moreover, legislative measures of the EU can be challenged on the grounds of fundamental rights and the Member States must ensure that the provisions are upheld by the private entities.[73] For the reasons mentioned above, it can be stated that there is an indirect, and sometimes a direct application of fundamental rights upon private entities, a so-called *horizontal application*.[74] Lastly, private entities operating on the internal market *digitally* may also be challenged for their failure to comply with EU privacy rights, as demonstrated in cases *Google Spain* and *GC and Others*.[75]

3. The right to Privacy and Personal Data in the EU

The right to privacy holds a significant position within the EU's legal system. The root of its importance derives from historical events where atrocities were facilitated through the collection and systematic abuse of personal information containing an individual's location, age, gender, profession, religion and ethnicity.[76] Following the atrocities, the Universal Declaration of Human Rights (UDHR) was adopted by the United Nations General Assembly in 1948 containing the right to privacy.[77] In Article 12 of the UDHR, it is stipulated that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence (…)"[78] This may be viewed as the first step in laying down privacy as a fundamental human right, as it laid the ground for the right to privacy in Article 8 of the ECHR and Article 7 of the EU Charter.[79] Notably, alongside the protection of privacy in Article 7 of the EU Charter, the right to protection of personal data is stipulated in Article 8 of the EU Charter.[80]

[72] Paul Craig and Gráinne de Búrca (n 21) 401.
[73] ibid.
[74] ibid, 419; Robert Schütze (n 15) 487.
[75] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317;Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés* [2019] ECLI:EU:C:2019:773.
[76] Jan Trzaskowski and Max Gersvan Sörensen, *GDPR Compliance – Understanding the General Data Protection Regulation,* (Ex Tuto Publishing A/S 2019) 42 – 45.
[77] ibid, 44. The abuse of personal information using technology led to the establishment of a system for the protection of human rights.
[78] United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III). <https://www.ohchr.org/en/human-rights/universal-declaration/translations/english> Accessed 31 March 2023.
[79] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16 (Springer Science & Business, 2014) 38.
[80] C-203/15 *Tele2 Sverige* [2016] ECLI:EU:C:2016:970, para 129. Despite embodying privacy in a sense similar to the ECHR, the EU has its own approach to the right to privacy with an internal market aspect. The explicit protection afforded to the right to personal data is not seen in the ECHR, making such protection unique to the EU.

3.1 The Right to Privacy and Personal Data: the EU's Combination of Economic and Fundamental Rights Approach

Due to a broad conceptual and theoretical understanding of the notion of 'privacy', case law under the ECHR became a powerful force in solidifying the legal notion of 'respect for private life'.[81] Since Article 7 of the EU Charter is mirrored after Article 8 of the ECHR, it is necessary to understand the pioneering case law on privacy, such as *Klass and Others v Germany* and *Malone v UK*, from the ECtHR.[82] In these cases, the scope of protection granted under Article 8 of the ECHR encompasses a person's private life, family life and their correspondence, including their communication and even DNA-profiles.[83] Building upon this importance given to privacy, the EU has drawn inspiration from the above mentioned cases of ECtHR on privacy in its own approach to protect the private life of individuals.[84]

At the same time, diverging approaches to privacy existed within the internal market in accordance with Member States constitutional norms, causing a potential obstacle to competition.[85] Subsequently, a framework which could secure 'privacy' as a fundamental right while *also* securing the economic approach for the internal market through harmonisation of privacy approaches was developed.[86] The key step towards the protection of personal data took place in 1990 as the European Commission adopted a package including proposals for the protection of personal data.[87] This proposal resulted in the adoption of Directive 95/46/EC (Data Protection Directive) in 1995 on the basis of Article 95 of the EC Treaty (now Article 114 TFEU).[88] The Data Protection Directive became the main privacy framework intended as a harmonisation tool enabling the free flow of data in the internal market as the economic approach, while also enshrining the right to privacy as a fundamental right.[89]

3.2 Case Law Shaping the Regulatory Environment on Privacy and Data Protection

Digital Rights

---

[81] Gloria Gonzalez Fuster (n 79) 38.
[82] *Klass and Others v Germany*, App no 5029/71 (ECtHR 6 September 1978) and *Malone v UK*, App no 8691/79 (ECtHR 2 August 1984).
[83] ibid, para 41;*Malone v UK* para 64; Mark Klamberg, 'Skydd enligt Europakonventionen om skydd för de mänskliga rättigheterna' in Cecilia Magnusson (ed), *Rättsinformatik* (Studentlitteratur AB 2016) 168.
[84]Case *Tele2 Sverige* (n 80), para 129; Joined Cases C-293/12 and C-594/12 *Digital Rights* [2014] ECLI:EU:C:2014:238, paras 54-55.
[85] Commission, 'On the protection of individuals in relation to the processing of personal data in the Community and information security' COM (90) 314 final, 2-4. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314&from=EN> Accessed 11 April 2023; Gloria Gonzalez Fuster (n 79) 55-71. Chapter 3 describes and compares diverging national approaches to privacy protection in the EU.
[86] ibid, 112-117 and 126; The first fundamental rights framework, Directive 95/46/EC, is established on the basis of Article 95 EC (now Article 114 TFEU).
[87] ibid, 124.
[88] Consolidated Version of the Treaty establishing the European Community [2000] OJ C 325 <https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A12002E%2FTXT> Accessed 11 April 2023.
[89] Gloria González Fuster (n 79) 124; Maria Tzanou, *The Fundamental Right to Data Protection, Normative Value in the Context of Counter-terrorism Surveillance* (Hart Publishing 2017) 16-17.

Digital Rights plays a prominent role for the normative context of privacy in the EU. In the case, Directive 2006/24/EC (Data Retention Directive) was scrutinised for its compatibility with the fundamental rights to privacy and right to personal information as it obliges telecommunication and internet service providers to retain a broad range of personal data concerning individuals without differentiation.[90] The CJEU elaborated that the gathering of location and traffic-data enabled by the Directive enables very precise conclusions to be drawn concerning a person's habits, movements, activities and social environment.[91] Since the Data Retention Directive enabled collection of information on *any* user without requiring prior warranty, justifications, limitations, or exceptions, it was deemed problematic due to its lack of safeguard from abuse.[92] It was therefore highlighted how such a broad and unrestricted collection of personal data affects not only Articles 7 and 8 of the EU Charter, but also Article 11 of the EU Charter concerning freedom of expression.

For these reasons, the CJEU found that the provisions allowed for an extensive retention of data without *clear* and *precise* rules to limit the extent of interference of the right to privacy and personal data.[93] This constituted a particularly serious interference with the fundamental rights of individuals, breaching Articles 7 and 8 of the EU Charter as it was not which was not strictly necessary to attain its objective, nor was it proportional.[94] Consequently, the Data Retention Directive was invalidated for its lack of sufficient safeguards to ensure effective protection of the data retained against the risk of abuse.[95] As Article 52(1) of the EU Charter stipulates that 'any limitation of the exercise of the rights and freedoms recognised by this Charter must (…) respect the essence of those rights and freedoms.', Maria Tzanou argues that case *Digital Rights* suggests that there are 'hard core' data protection principles in the form of 'essence' that should not be violated.[96]

Schrems and Tele2 Sverige

Although case *Schrems* focuses on data transfer to a third country (the US), it is worthy to understand where the emphasis is put in the doctrine of privacy.[97] In *Schrems*, the CJEU assessed whether the 'Safe Harbour Privacy Principles' could guarantee an adequate level of privacy and data protection as the EU's legal frameworks.[98] The CJEU invalidated the Safe Harbour Privacy Principles and confirmed yet again, that the *general* storage of data '*without differentiation, limitation or exception being made in the light of the objective pursued*' while allowing public authorities to access the stored data in such a manner interferes with the right

[90] *Digital Rights* (n 84), paras 57-68.
[91] ibid, paras 27-29; Maria Tzanou (n 89) 59.
[92] *Digital Rights* (n 84) paras 57-68.
[93] ibid, para 65.
[94] ibid, paras 66 and 69. The objective of Data Retention Directive was to harmonise obligations on providers for the investigation, detection and prosecution of serious crimes, see Recital 21 of the Data Retention Directive <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024> Accessed 6th April 2023.
[95] ibid, paras 66, 69 and 73.
[96] Maria Tzanou (n 89) 42-43.
[97] Case C-311/18 - *Facebook Ireland and Schrems (Schrems)* [2020] ECLI:EU:C:2019:1145.
[98] ibid, para 94.

to the essence of privacy.[99] This approach seems to follow Advocate General Bot's opinion where access to the *content* of private data would automatically lead to an interference with the essence of the fundamental right to private life.[100]

Continuing the subject of data-gathering of the *content* of electronic communications, the CJEU's view on the protection of privacy and personal data also extends to 'non-content data' as clarified in case *Tele2 Sverige*.[101] Non-content data, also referred to as metadata, can be described as 'data about data'. It is essentially information about communication traffic including locations, volume, directions, numbers, or addresses. In the view of the CJEU, an analysis of metadata can reveal a large amount of sensitive information which could be used to construct a detailed profile of an individual's beliefs and behaviours using electronic communication systems.[102] Nevertheless, in *Tele2 Sverige*, Sweden was transposing the annulled Data Retention Directive. The relevant question concerned whether Directive 2002/58 (Electronic Communications Directive) prohibits national legislations from allowing indiscriminate data-collection of traffic and location data, in all modes of electronic communications on all users.[103] In its preliminary ruling, the CJEU seems to imply that metadata is as sensitive as content-data.[104] Due to its sensitive nature, the CJEU ruled that national legislation allowing *indiscriminate* collection of metadata is a serious interference of the fundamental right to privacy.[105] Therefore, given the seriousness of the interference in the fundamental rights, national legislations enabling retention of metadata can only be justified by the objective of fighting *serious* crimes.[106] To that, the CJEU stipulates that such a measure must be based on objective evidence where the acquired metadata reveals a link, at least an indirect link, to *serious* criminal offences.[107]

Google Spain

Another important feature of the EU's privacy approach is the exercise of the right to be forgotten. In case *Google Spain*, a Spanish national (Mr Costeja González) lodged a complaint against a newspaper publisher in 2010. The complaint concerned the fact that the applicant's name appeared in links on the search engine (Google), mentioning a real-estate auction tied to proceedings for the recovery of social security debts from 1998. Mr Costeja González thus requested the publisher to remove or alter those pages mentioning his name to no longer display

[99] ibid, para 93.
[100] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:627, Opinion of AG Bot, para 177; *Digital Rights* (n 84) para 39.
[101] *Digital Rights* (n 84) paras 26-29; Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864, 879. 'Content data' is the content of communication or information. 'Non-content data' is thus data *about* data, such as volume, storage location or duration. Non-content data is also referred to as 'metadata'.
[102] Nora Ni Loideain 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' 54 in James Schwoch, John Laprise and Ivory Mills, Surveillance: Critical Analysis and Current Challenges, Media and Communication (2015) vol 3, 53, 54.
[103] *Tele2 Sverige* (n 80) para 62.
[104] ibid, para 99.
[105] ibid, paras 99–100; Maja Brkan (n 101) 873.
[106] *Tele2 Sverige* (n 80) para 111.
[107] ibid, para 111.

it upon a search using Google. The complaint was rejected by the Spanish Data Protection Agency (AEPD) but was upheld against Google Spain and Google Inc. It was therefore brought before the national court and later referred to the CJEU as the AEPD raised questions regarding the obligations on operators of search engines. The CJEU thus assessed whether a data subject has the right to erasure and whether a search Google had an obligation under the Data Protection Directive to remove links displaying Mr Costeja González data.

The CJEU reiterated that the search engine *governs* the processing of personal data liable to particularly infringe the right to privacy, both of which are subject to Article 7 and 8 of the EU Charter. The CJEU therefore considered that data subjects indeed have a right to erasure while also clarifying limitations. Moreover, the CJEU considered balancing of opposing rights and interests connected to the right to erasure. Regarding the balancing of rights and interests, the CJEU held that the general rule to the rights of the data subjects is that privacy and data protection override the public interest of internet users having access to information, as well as economic interests.[108]

3.2.1 Outcome of CJEU-cases building upon privacy norms in the internal market

In the above mentioned cases, rulings of the CJEU's emphasises the protection of privacy rights in a manner similar to the protection of privacy granted by the ECtHR's interpretation of Article 8 ECHR. The recurring themes of EU privacy can be summarised as requiring clear and precise safeguards to limit the extent of interference of the right to privacy and personal data when extensive retention of data is gathered about individuals. It is also clear in cases *Tele2 Sverige* and *Schrems* that the general storage of data without differentiation, limitation or exceptions for the objective pursued, interferes with the essence of privacy. *Tele2 Sverige* also establishes the requirement of an indirect link to serious crimes warranting the retention of data which can be used to construct a detailed profile about an individual (non-content data). Case *Digital Rights* also clarifies the distinction between the right to privacy and the right to personal data, showcasing the independent reasoning for the right to personal data in Article 8 of the EU Charter, while emphasising its interconnectedness to Article 7 of the EU Charter.[109]

3.3 The General Data Protection – Concretising the Right to Personal Data in the Internal Market

In contemporary times, the Data Protection Directive is repealed by Regulation 2016/679, commonly referred to as the General Data Protection Regulation (GDPR) adopted in 2016.[110] Some of the outcomes of EU privacy cases are now reflected in integral concepts of the GDPR, which include 'personal data' (information about a person which can be used to identify that person), 'processing' personal data, and 'lawfulness' of data processing.[111] Importantly,

[108] Maria Tzanou (n 89) 62.
[109] ibid, 58.
[110] Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119. (Hereinafter 'GDPR').
[111] Article 5 and Recital 39 of the GDPR: Article 4(2) provides a definition of 'processing', which essentially means any operation or set of operations which is performed on personal data or on sets of personal data.

individuals whose data are being processed (data subjects) are entitled to rights under the GDPR. Some of these rights include the right to transparent information, the right of access to the information collected about them and the right to be forgotten (also referred to as right to erasure) stipulated in Article 17 of the GDPR.[112] The GDPR also contains obligations for private and public entities to facilitate the exercise of the rights of data subjects when processing their personal data.[113] In its Article 5, the GDPR establishes principles of fairness, lawfulness, transparency, purpose limitation, data minimization and accuracy when processing personal data.[114] Essentially, these principles require the entity which is processing personal data (the processor) to fulfil obligations to protect the personal information of data subjects from misuse, accidents or any other irregularities. Particularly, the data subject must be made aware that data about them is being processed, as well as be made aware of risks, safeguards and rights connected to their personal data.[115]

Importantly, the GDPR stipulates that the purposes for the processing must be specific and explicit, as well as determined at the time of the collection. The personal data must also be relevant for that specified purpose and limited to what is necessary to achieve it. In connection to the purpose limitation, a limitation of time for the processing must be established where a periodic review and erasure is carried out.[116]

3.3.1 Sensitive information warranting additional protection

Another important aspect of the GDPR is the notion of special categories of personal data, which essentially recognises the sensitive nature of certain personal information (such as ethnic origin or medical information) which could affect a person's fundamental rights and freedoms.[117] In particular, 'sensitive data' are described in the GDPR as particularly sensitive in relation to fundamental rights and freedoms, thereby meriting specific requirements in the context of their processing. In addition to specific requirements for the processing of sensitive data, derogations must be explicitly provided. Another way of processing sensitive data is through obtaining the data subject's explicit consent.[118] Examples of sensitive data are stipulated in Article 9(1) of the GDPR as:

> (…) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (…).[119]

[112] Articles 12 – 15 GDPR enshrines the right to transparency and the right of access; Recital 65 and Recital 68 GDPR elaborates that the right to be forgotten is an important strengthening of data subject's rights and control over their own information in the online environment.
[113] Recital 65.
[114] Article 5 of the GDPR.
[115] Recital 39 of the GDPR.
[116] ibid.
[117] Recital 51, Recital 75, and Article 9 GDPR.
[118] Recital 51 GDPR.
[119] Article 9(1) GDPR.

Nevertheless, according to the GDPR, the context of the processing of sensitive data could create significant risks to the fundamental rights and freedoms of a person and is thus prohibited to process without specific protection.[120] Such risks may involve consequences such as discrimination, identity theft, fraud, financial loss or social disadvantage which could occur. Importantly, processing of sensitive data could aggravate the severity of those consequences especially where processing involves a large amount of personal data and affects a large number of data subjects.[121]

Moreover, to lawfully process personal data relating to criminal convictions and offences, Article 10 of the GDPR requires the control of official authority or authorisation by EU or Member State laws which provide appropriate safeguards for the rights and freedoms of data subjects. Therefore, analysing and processing data concerning criminal convictions or offences, where personal aspects regarding a person's economic situation, reliability, or behaviour to create a profile, risk interfering with a person's rights and freedoms without adequate safeguards.[122] Member States may however restrict certain provisions within the GDPR for the purposes of the prevention, investigation, detection, or prosecution of criminal offences.[123] Nevertheless, the processing of sensitive data is subject to specific processing conditions.[124]

3.3.2 The Law Enforcement Directive

When it comes to the processing of personal data by law enforcement agencies for the purpose of crime prevention, investigation, detection or prosecution of criminal matters, such processing falls outside the scope of the GDPR.[125] Instead, the GDPR refers to the *lex specialis* for data-processing in the context of criminal matters – Directive 2016/680 or the 'Law Enforcement Directive (LED).[126] According to Article 3(7)(a) LED, 'competent authorities' includes any *public* authority competent for the law enforcement purposes.[127] Data transfers from private entities on behalf of law enforcement agencies are subject to the LED.[128]

Aside from the possibility of granting private entities broader investigative powers under the LED, the rights of data subjects under the LED can be restricted to a greater extent, as opposed to rights guaranteed by the GDPR. This is motivated to 'avoid obstructing official or legal inquiries, investigations or procedures'.[129] Another difference from the GDPR found in the

[120] Recital 51.
[121] Recital 75 GDPR.
[122] Recital 75 GDPR.
[123] Article 23 GDPR.
[124] Recital 51 and 56 of the GDPR.
[125] Article 2(d) GDPR states that the GDPR is inapplicable when 'competent authorities' processes data in the context of crime prevention, detection and investigation.
[126] Council Directive (EU) 2016/680 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 [2016] OJ L 119. Hereinafter 'LED'. See Article 1 of the LED.
[127] Purposes which enable a competent authority to processing personal data is listed in Article 1(1) of the LED.
[128] Recital 11, LED.
[129] Article 13(3) of LED.

LED is that law enforcement agencies are allowed to process personal data for the *detection* of crime, as opposed to the principle of purpose limitation in the GDPR where a specificity of purpose for the data processing must be defined before processing.[130] Considering the differences in data protection rights between the GDPR and the LED, the scope of LED entails a broad discretion to process personal data.[131]

Although the GDPR and the LED mainly refer to the processing of personal data, it is evident that there is a strong link between personal data and the importance given to the right to privacy. The manifestation of the right to privacy as enshrined in the EU Charter can also be seen in the additional protection afforded to the special categories of data which are regarded as particularly sensitive and interconnected with the rights and freedoms of a person.[132] Therefore, in the context of the EU, both the right to privacy and right to personal data are vital for the understanding of the normative efforts within the internal market.[133]

4. Organised Crimes and Terrorist Financing: an Exploitation of The Internal Market

Despite the successful facilitation of cross border commercial activity alongside the guarantee of fundamental rights in the internal market, certain challenges have emerged in times of economic uncertainties. For instance, organised crimes have become one of the most serious challenges to the security within the EU.[134] Of particular concern is the highly adaptive and sophisticated nature of organised networks, operating in wide, cross-border constellations which are intertwined with the legitimate economy.[135] Payment solutions, digital marketplaces and platforms become part of the various means to conduct criminal activities. At the same time, billions of euros generated from criminal activities are poured into the EU's economy.[136] Other than the use of digital solutions, criminal organisations often infiltrate the licit economy through businesses vulnerable to pressure.[137]

4.1 Legitimate Businesses and Their Hands in Financial Crimes

According to a 'Serious and Organised Crime Assessment' (SOCTA) published by Europol in 2021, all organised crimes make use of legitimate business structures for its veil of

[130] Recital 12, LED.
[131] Nadezhda Purtova 'Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships' (2018) Vol. 8 International Data Privacy Law 52, 60-61; Recital 12 of the LED.
[132] Recital 4 GDPR; Articles 7 and 8 of the EU Charter enshrines the right to private life and personal data.
[133] *Tele2 Sverige* (n 80) para 129; Maria Tzanou (n 89) 59; *Digital Rights* (n 84) paras 29 and 36. Article 8 of the EU Charter is viewed as a fundamental right distinct from Article 7 EU Charter. It is examined independently from the right to privacy in Article 7 of the EU Charter.
[134] SOCTA (n 2) 14 and 15.
[135] ibid, 14.
[136] ibid, 15.
[137] Commission, 'on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities' (Commission staff working document – Accompanying the document report from the commission to the European Parliament and the Council) (2022) SWD (2022) 344 final, 17.

legitimacy.[138] Examples of such businesses are hotel, retail, gastronomy, and real estate-businesses, some of which were particularly affected by travel restrictions imposed during the Covid-19 pandemic. Due to the reduced prices in properties and financial difficulties resulting from lock-down measures, these sectors became particularly susceptible to criminal exploitation.[139] For the real-estate sector, unreported cash payment is as prevalent as the creation of obscure construction firms where illegal workforce and low paid staff are used to under-declare costs. With the help of different stakeholders such as architects, construction workers and construction site managers, faulty declaration of payments or invoice falsification is conducted to help criminal organisations conceal the origin of their illegal proceeds.[140]In other words, financial crimes are often facilitated through the abuse of legitimate businesses.[141] This intertwining of licit and illicit businesses creates a difficulty for law enforcement to detect and investigate criminal activities.

4.1.2 Financial crimes through obscurities guaranteed by FinTech services

Since financial crimes are an integral part of organised crimes for being highly profitable and hard to detect, it also functions as key facilitation to terrorism.[142] Adding to the complexity of detecting financial crimes is the emergence of technical innovations in banking which has contributed to convenience, usability, and instantaneous transactions.[143] In the EU, financial technology (FinTech) solutions are increasingly becoming a norm among consumers, with a 50% increase in mobile banking since the end of 2019.[144] Similarly, new ways of money transferring are developing in a pace ungraspable by legal mechanisms, creating a regulatory vacuum concerning new methods of transferring money.[145] These new Fintech services are online platforms and applications, network-based transaction technologies for example. Some examples of payment services used for money transfer are Western Union or MoneyGram. Another method of transferring money is through digital currencies and cryptocurrencies which ensure a high level of anonymity.[146]

Importantly, these new payment products and services are not traditional financial service providers such as banks, meaning that they can provide most of the functionalities of a bank in terms of transactions and handling of funds, but they do not always carry the same

[138] SOCTA (n 2) 24. These facades of legitimate businesses are also referred to as 'front' or 'shell' companies.
[139] SWD (2022) 344 (n 137) 17.
[140] ibid.
[141] SOCTA (n 2) 24.
[142] Europol, 'Enterprising criminals, Europe's fight against the global networks of financial and economic crime' (2020) Europol <https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime> Accessed 21 May 2023, 19.
[143] ibid, 7.
[144] ibid. FinTech companies offer financial services with the use of digital applications.
[145] ibid; Europol, 'Terrorism Situation and Trend Report' (TESAT) (2022) Europol <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat> Accessed 21 May 2023, 18.
[146] ibid, 19.

responsibilities of a bank.[147] Therefore, when it comes to Fintech, authorities are facing challenges when developing approaches and mechanisms to prevent and detect money laundering.[148] Banking services and digital solutions are often abused by nearly all criminal networks. Consequently, hundreds of financial crime investigations are carried out every year in the EU while law enforcement authorities are faced with great difficulties in detection and investigation, leading to the application of intrusive measures aimed at increasing transparency and traceability of the funds.[149]

4.1.3 Terrorist organisations and its diversified funding sources - intentional and unintentional funders of the EU

According to Europol's assessment, criminal groups and terrorists hold divergent core motivations where organised criminals seek profits and terrorists pursue political or ideological aims.[150] Despite such differences however, certain overlapping interactions are prevalent between the groups. For instance, terrorists are often involved in serious and organised crime to finance and expand their terrorist activities.[151] The groups may share the same sources for the purchasing of weapons, forged documents, potential recruits, and finances, with most overlapping occurring through financial transactions.[152] Thus, it is evident that organised criminal networks offer services to terrorism, while in some cases, terrorists are involved in the organised crime themselves, or have connections to the criminal network in order to fund terrorism. Nevertheless, the denominating nexus between organised crime and terrorist groups is profit-making, where the EU is the ground for which profitable criminal activities are carried out.[153]

Moreover, terrorist attacks in 2015 to 2021 have uncovered the means of terrorism financing.[154] In a terrorism situation and trend-report by Europol, donations are highlighted as one of the prominent means of funding terrorist organisations across the EU.[155] While some of the donations are intentionally given in support of terrorist activities, some donations are collected through the guise of charity organisations.[156] In Spain, three individuals were arrested for funding al-Qaeda, as donations were obtained under the guise of humanitarian aid for Syrian

[147] Enterprising criminals (n 132) 7. Increased digitalisation without interaction with customers weakens procedures banks are under obligation to comply with for the prevention of tax fraud, money laundering, and online banking fraud.
[148] ibid, 16-17.
[149] ibid.
[150] SOCTA (n 2) 25.
[151] TESAT (n 145) 19. For example, some criminal gangs subscribe to right-wing extremism, such members have been found cooperating with right wing terrorist groups.
[152] ibid, 19. SOCTA (n 2) 25.
[153] TESAT (n 145) 20; Commission, 'on the EU Strategy to tackle Organised Crime 2021-2025' (2021) COM(2021) 170 final, 1; Commission, 'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework' (2019) COM(2019) 360 final, 1.
[154] Nikola Paunovic, 'Terrorist Financing as the Associated Predicate Offence of Money Laundering in the Context of the New EU Criminal Law Framework for the Protection of the Financial System' (2019) 3 ECLIC 659, 660; TESAT (n 145) 17.
[155] TESAT (n 145) 17.
[156] ibid.

orphans by a religious organisation.[157] Other means of donations can occur through the availability of the Internet and increasing abundance of crowdfunding websites which facilitates donations from a large number of donors across the globe.[158] Moreover, fund-collection can be conducted through campaigns uploaded on platforms such as Patreon, YouTube, GoFundMe, whereas popular internet payment systems are used for the transactions. Like criminal networks, terrorist organisations also utilise these legitimate E-commerce-platforms for sale of goods.[159]

Aside from businesses, terrorist organisations may also commit various types of fraud such as tax fraud, tax evasion, social benefit fraud, loan fraud and insurance fraud. More criminal activities conducted by terrorist organisations include trafficking, sale of drugs, robberies, thefts, and extortions among others, all of which carried out within the internal market.[160] The flow of illicit money harms the international development of the EU's financial sector as criminals and financiers of terrorism could take advantage of freedom of capital movements and the freedom to supply financial services guaranteed within the internal market of the EU.[161] Not only does criminal exploitation of the financial system allow terrorism and organised crime to expand within the internal market, but it also causes losses to public revenue.[162] The infiltration into licit businesses puts business sectors at risk and threatens financial institutions operating in the EU's economy. Through the exploitation of businesses and bribery of politically exposed persons or persons in sectors such as healthcare, pharmaceuticals, construction, education, the free-market environment is undermined.[163]

5. The legal landscape of anti money laundering and terrorist financing

For an effective cooperation and creation of the AML-regime within the EU and its Member States, the recommendations, and guidelines of the Financial Action Task Force's (FATF) is complied with for an effective cooperation between EU bodies and national authorities as well as private entities.[164] The FATF is established by the international Group of Seven (commonly referred to as G7) to provide expertise on money laundering.[165] Through examining trends, researching and developing measures, the FATF issues recommendations on AML-measures

[157] ibid.
[158] ibid.
[159] ibid, 18.
[160] ibid, 18.
[161] Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May [2015] on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141, Recital 2.
[162] SOCTA (n 2) 26.
[163] ibid.
[164] Commission, 'on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' (2020) 2020/C 164/06, 2. Hereinafter referred to as 'the Action Plan'.
[165] FATF, 'History of the FATF' <https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html> Accessed 18 February 2023; G7, also referred to as 'the group of 7' is a political forum consisting of Canada, UK, Germany, Italy, the US, France, Japan and the EU, see more at G7, (www.g7germany.de 2023) <https://www.g7germany.de/g7-en/g7-summit/g7-members> Accessed 18 February 2023.

to states and entities which are members of the FATF. After one year of its establishment, the FATF issued 40 Recommendations which specified legal, regulatory, and operational measures for countries to rely on in the detection, prevention, and punishment of money laundering.[166] Monitoring was also a part of the FATF's tasks. By 2001, its mandate expanded to cover financing of terrorism.[167] In short, the FATF produces guidance, Best Practice Papers, and advice with the aim to assist its international network with the implementation of FATF standards to prevent money laundering and financing of terrorism.[168]

5.1 EU Bodies in the Fight Against Money Laundering and Terrorist Financing

At the EU level, the EU Commission monitors the implementation of the AML-rules across Member States, which could result in country specific recommendations issued by the EU Council. The EU Commission provides technical support where shortcomings are found.[169] Member States failing to transpose the AML-Directives would be subject to infringement proceedings imposed by the EU Commission.[170] The European Bank Association (EBA) is tasked to lead, coordinate and monitor the financial service providers and financial supervisory authorities compliance with AML-measures within Member States.[171] Another important body is Europol which acts as the EU criminal information hub, which cooperates with Member States' police forces through information exchanges and threat assessments. When it comes to the cooperation between police and private parties and the processing of large datasets, Europol's competences and tools were strengthened to handle such operational needs through new competences granted by the EU Commission.[172]

At the national level, national financial intelligence units (FIU) play an integral role in the AML-regime as it is tasked to investigate and prevent money laundering and terrorist financing.[173] Finally, financial service providers and certain private entities are part of the AML-regime as they are obliged to document information, monitor transactions and report any suspicious activities to their national FIUs.[174] However, since obliged entities are private entities, there is usually a lack of expertise and experience in detecting criminal activities. Therefore, the AML-framework has strengthened the role of the public sector in providing obliged entities with guidance on money laundering and terrorist financing.[175] The cooperation

[166] FATF, 'Financial Action Task Force – 30 years', FATF (2019) <www.fatf-gafi.org/publications/fatfgeneraldocuments/FATF-30.html> Accessed 18 February 2023, 10-11.
[167] ibid, 11.
[168] FATF, 'History of the FATF' <https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html> Accessed 18 February 2023.
[169] The Action plan (n 164) 3.
[170] ibid; Article 51 4th AML-directive.
[171] The Action plan (n 164) 3.
[172] COM(2021) 170 final (n 153) 6; Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L 169.
[173] Recital 37 of the 4th AML-directive.
[174] Articles 11, 13 and 14 of the 4th AML-directive.
[175] Benjamin Vogel, 'Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing' [2022] The European Criminal Law Associations' Forum, 'The Prevention and Fight

between the private obliged entities and the public authorities is argued to encourage obliged entities to demonstrate that they undertook adequate steps to implement the AML-measures to avoid public sanctions.[176]

5.2 EU's Harmonisation of Diverging Approaches in Tackling Financial Crimes

In a report by Europol in 2017 it was revealed that approximately 0.7-1.28% of the EU's annual GDP has been 'detected as being involved in suspect financial activity'.[177] As a reaction to the findings, the EU Commission adopted the communication 'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework' (hereinafter the 'Communication') aimed at improving supervision at an EU level while also strengthening coordination between EU Member States' FIUs. Specifically, the Communication focused on the harmonisation of AML-approaches which varied across Member States.[178] Accompanying that Communication, four accompanying reports were issued to highlight the risks of money laundering in different sectors across the EU and their vulnerabilities, shortcomings in the cooperation and supervision.[179]

In one of the reports, the 'Supranational risk assessment report' it is elucidated that diverging national approaches on cash-payments distorts competition in the internal market since cash-intensive businesses could relocate across borders.[180] Another issue raised about cash-payments concerns different legislations on cash-limitations, where perpetrators could circumvent restrictive rules in one Member State and invest in a cash-intensive business in another Member state with permissible rules on cash limitation. This legislative fragmentation among the Member States' is viewed as one of the enabling factors for terrorist activities to be carried out through moving to Member States with weaker restrictions.[181]

Following the Communication and the issues highlighted in the accompanying reports, the EU Commission was invited by the EU Parliament and the EU Council to investigate how

against Money Laundering – New Trends' 1st edition <https://eucrim.eu/issues/2022-01/> Accessed 22 May 2023, 52.

[176] ibid, 53.

[177] Europol Financial Intelligence Group,'From suspicion to action, converting financial intelligence into greater operational impact' (2017) Publications Office of the European Union <https://www.europol.europa.eu/publications-events/publications/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> Accessed 16 February 2023, 26.

[178] EU Commission, 'EU context of anti-money laundering and countering the financing of terrorism' (www.finance.ec.europa.eu) <https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en> Accessed 18 February 2023; COM(2019) 360 final (n 153); EU Commission, 'Questions and Answers - Commission steps up fight against money laundering and terrorist financing' (www.ec.europa.eu, 7 May 2020) <https://ec.europa.eu/commission/presscorner/detail/eng/qanda_20_821> Accessed 18 February 2023.

[179] EU Commission, 'Fight against money laundering and terrorist financing: Commission assesses risks and calls for better implementation of the rules' (www.ec.europa.eu, 24 July 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452> Accessed 18 February 2023. These four reports include the 'Supranational risk assessment report', the 'Assessment of recent high-profile money laundering cases in the financial sector', the 'Financial Intelligence Units report', and the 'Interconnection of central bank account registries report'.

[180] (2022) SWD (2022) 344 final (n 137) 16.

[181] ibid, 19; The Action Plan (n 164) 4-5.

international cooperation across the EU could be achieved.[182] The investigation resulted in the issuance of an Action Plan alongside other instruments in 2020 to strengthen the efforts against money laundering and terrorism financing across the EU.[183] In the EU's Commission's Action plan, money laundering is deemed detrimental to the EU's economy, good governance, and the financial system as a whole, which in turn undermines trust and investor confidence when reputation is harmed.[184] Due to the risks mentioned above, financial crimes and the financing of terrorism is viewed as a major threat to the integrity of the EU's financial system by the EU Commission, therefore, rigorous efforts have been made to strengthen the legal frameworks.[185] Therefore, on 20th July 2021, the EU Commission adopted a package of legislative proposals to tackle money laundering, including a proposal to create a new EU authority for AML and a proposal for an EU regulation.[186]

Evidently, great efforts have been made at the international level, EU level and national level to counter financial crimes and terrorist financing. With the emergence of new tech, regulatory frameworks must adequately address and capture the highly innovative nature of both organised crimes (including terrorist activities) and NPPS alike.[187] Adding to the challenges is the cross-border nature of financial crimes, meaning that measures adopted by the EU must consider international coordination and cooperation.[188] Aside from the regulatory complexities, law enforcement authorities are faced with crimes which are complex to investigate, detect and prevent. In consideration to the difficulties highlighted above, far-reaching measures have been included in the creation of a legal framework.[189]

5.3 Directive 2015/849 (4th AML-directive) – Emphasising Risk Assessment and Due Diligence

In 2012, the EU Commission undertook the task to review the 3rd AML-directive (Directive 2005/60/EC). At the same time, FATF conducted a revision of its own Recommendations. The outcome of both FATF and EU Commission's review elucidated the necessity of an improved AML-regime, due to the emergence of new threats in the financial market and shortcomings in

[182] The Action Plan (n 164) 4-5.
[183] EU Commission, 'Questions and Answers - Commission steps up fight against money laundering and terrorist financing' (www.ec.europa.eu, 7 May 2020) <https://ec.europa.eu/commission/presscorner/detail/eng/qanda_20_821> Accessed 18 February 2023; The Action Plan (n 164).
[184] The Action Plan (n 164) 3; Recital 1 of the 4th AML-directive.
[185] COM(2019) 360 final (n 153) 1.
[186]Commission, 'Anti-money laundering and countering the financing of terrorism legislative package' (finance.ec.europa.eu 2021) < https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en> Accessed 21 April 2023; Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 [2021] COM(2021) 421 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420> Accessed 21 April 2023.
[187] COM(2019) 360 final (n 153) 1. NPPS (New payment products and services).
[188] Recital 4 of the 4th AML-directive.
[189] SOCTA (n 2) 14-15. In the report, far-reaching methods have been described as successful for the prevention of money laundering.

the 3rd AML-Directive.[190] The establishment of the 4th AML-directive in 2015 is therefore partly driven by a review of the 3rd AML-Directive at the EU level, and partly by a FATF-revision of its own Recommendations internationally.[191] Through the introduction of new measures and requiring stricter control measures by private entities, the adoption of the 4th AML-directive was aimed to strengthen international cooperation and harmonise AML across the EU.

The 4th AML-directive also expanded the scope of 'obliged entities'. Obliged entities are private entities which are required to conduct AML-measures to detect money laundering and terrorist financing. Article 2 of the 4th AML-directive lays down some examples of obliged entities, which include credit institutions, financial institutions, tax advisors, notaries and other legal professionals carrying transactions concerning real properties. These are largely entities which provide payment services, however, other obliged entities are those which trade goods where payments made or received are in cash and reaches an amount of 10 000 EUR or more, whether the transaction is carried out in a single operation or in several operations.[192] The 4th AML-directive expanded the scope of obliged entities by including providers of gambling services and other entities that must conduct AML-measures subject to 4th AML-directive.[193]

5.3.1 Systematic risk-based approach

The 4th AML-directive emphasises a risk-based approach which requires obliged entities to carry out risk assessments where the level of actions depends on the severity of the risks of money laundering.[194] Moreover, Member States as well as obliged entities must conduct regular risk assessments.[195] Member States' national risk assessments must provide information on high risk and low risk sectors for money laundering and terrorist financing.[196] The aim of the risk assessment is for each Member State to identify, assess, understand and mitigate those risks. Furthermore, the risk assessment must be published and made accessible for obliged entities to use as guidance and through such, the obliged entities can understand and manage their own risks.[197]

[190] Harold Koster, 'Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework' (2020) Vol 23. 2 Journal of Money Laundering Control 379. <https://www.emerald.com/insight/content/doi/10.1108/JMLC-09-2019-0073/full/pdf?title=towards-better-implementation-of-the-european-unions-anti-money-laundering-and-countering-the-financing-of-terrorism-framework> Accessed 22 May 2023, 380.
[191] Harold koster (n 190) 380; Commission, 'on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' [2012] COM/2012/0168 final.<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52012DC0168> Accessed 21 April 2023.
[192] Article 2(1)(e)-(f), Article 11(b)-(c) of the 4th AML-directive. In these Articles, it is clear that the list of obliged entities which must carry out these due diligence measures is non-exhaustive and includes non-financial entities depending on the amount of transactions carried out.
[193] Article 2(1)(f) 4th AML-directive.
[194] Harold Koster (n 190) 380.; Article 2 of the 4th AML-directive.
[195] Article 7-8 of the 4th AML-directive.
[196] ibid, Article 7(1)-(4).
[197] ibid, Article 8(1)-(5).

Risk assessments carried out by obliged entities on their own customers are in a sense more in-depth, as it is aimed at identifying whether specific customers are likely to be involved in money laundering or terrorist financing. Some factors that are taken into consideration for such a risk assessment concern the country or geographical area the customer is based in, type of products, services, or sectors which could be prone to corruption and money laundering.[198] Some examples of high-risk sectors include cash-intensive businesses, dealers in precious metals, or pharmaceuticals.[199] Other risk factors could be the customer's reputation, nature and behaviour which could have links to high-risk sectors. Nevertheless, in assessing risk factors about the customer, the obliged entity is entitled to gather information from media reports and 'other sources of information' about the customer to find allegations of criminality or terrorism.[200]

The risk assessments conducted by obliged entities must be documented, up-to-date and made available to financial authorities.[201] The objective of risk assessments is to ensure that the obliged entity is identifying, understanding, and actively mitigating the risks of money laundering and terrorist financing.[202]

5.3.2 Obligation to conduct due diligence

Obliged entities must conduct due diligence on their customers (natural or legal person), which entails gathering information about the customer (natural person) or its beneficial owner for legal persons *before* a business relationship is entered, or when it is appropriate.[203] In Article 13 of the 4th AML-directive, it is stipulated that customer due diligence measures shall comprise of verification of a customer's identity, assessing and obtaining information on the purpose and nature of the business relationship, obtaining information on the source of the funds and scrutinising the transactions throughout the whole business relationship.[204] Aside from the obligation to conduct customer due diligence when establishing a business relationship and transactions exceeding a certain threshold, Article 11 of the 4th AML-directive stipulates that obliged entities must apply customer due diligence when there is a suspicion of money laundering. Customer due diligence measures are also prompted *regardless* of any derogation, exemption, or threshold of suspicion. It is therefore enough that there are *doubts about the veracity or adequacy* of the customer identification data.[205]

---

[198] ibid, Article 8; European Banking Authority 'Guidelines on on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849' [2021] EBA/GL/2021/02, 26-27. <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final Report on Guidelines on revised ML TF Risk Factors.pdf> 26 Accessed 30 April 2023. Hereinafter referred to as 'the EBA guidelines'.

[199] ibid.

[200] ibid, 28.

[201] Article 8(2) 4th AML-directive.

[202] ibid, Article 8(3).

[203] ibid, Article 14(1)-(2) and Article 14(5). Appropriateness of performing customer due diligence is depending on the circumstances in each case, for example, when there is a customer change or there are doubts about the veracity or adequacy of the information, see Article 11 of the 4th AML-directive.

[204] ibid, Article 13(1)-(4).

[205] ibid, Article 11(e)-(f).

Moreover, there are defined situations where the customer is at greater risk for money laundering or terrorist financing.[206] One example of greater risk is when the customer is based in a high risk third country as defined by the EU Commission or the Member State, or when the beneficial owner is a 'politically exposed person' (PEP). A PEP is a 'natural person who is or has been entrusted with prominent public functions'.[207] The scope of who may be defined as PEP includes heads of state, government, and ministers.[208] It also includes members of governing bodies of political parties and even members of supreme courts and more. In short, it includes people in position to exercise public powers.[209] Relatives and close associates are also considered as part of PEP.[210] Nevertheless, a situation involving a high-risk third country or a PEP is always considered high risk for money laundering and terrorism financing. Such a high-risk situation requires the obliged entity to carry out enhanced due diligence measures under Article 18(2) of the 4th AML-directive where they must examine, as far as reasonably possible, the background and purpose of unusually large and complex transactions, as well as increase monitoring of the business relationship. In short, the 4th AML-directive stipulates that the obliged entity is required to apply customer due diligence measures and where high-risk is deemed, enhanced customer diligence.[211]

5.3.3 Reporting to Financial Intelligence Units

Article 32(1) of the 4th AML-directive requires all Member States to establish a FIU to prevent, detect and combat money laundering and terrorist financing.[212] FIUs must cooperate with each other to the greatest extent possible, regardless of their organisational status, as FIUs may be law enforcement authorities in some Member States and some administrative.[213] Obliged entities must promptly inform the FIU and provide all necessary information upon the FIUs request upon detection of any suspicious activity which could indicate money laundering.[214] Additionally, Article 39(1) in the 4th AML-directive prohibits disclosure of information, where obliged entities are prohibited from disclosing any information about the report or investigation to the customer suspected of money laundering or terrorist financing.[215] When it comes to the national FIUs duties, it must exchange all information concerning money laundering or terrorist financing to another Member State's FIU if that information is requested for processing or analysis.[216]

[206] ibid, Article 18.
[207] ibid, Article 3(9).
[208] ibid, Article 3(9)-(11).
[209] ibid, Article 3(9)(a)-(h).
[210] ibid, Article 3(9)-(11).
[211] Article 20(b) of the 4th AML-directive.
[212] Recital 37 of the 4th AML-directive.
[213] Article 52 of the 4th AML-directive; Foivi Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive' (2020) Vol. 11(3) NJECL 351, 354. Some Member States may have established their FIUs as an administrative entity rather than a law enforcement entity like in some other Member States.
[214] Article 33(1)-(2) 4th AML-directive.
[215] ibid, Article 39(1).
[216] ibid, Article 53(1).

Another integral task of the Member State's respective FIUs is to receive obliged entities' reports of suspicious transactions. In their reports, all data relevant for the investigation of money laundering and terrorist financing is shared with their national FIUs.[217] FIUs thus have access to financial, administrative and law enforcement-information necessary for the investigation.[218]

5.4 Directive 2018/843 (5th AML-directive) – Demanding Transparency through Scrutinising Cryptocurrencies

In 2018, the 5th AML-directive was adopted to further capture new technologies which were not adequately addressed by the AML-regime. It modified the 4th AML-directive through introducing measures particularly targeting cryptocurrencies and service providers of such.[219] Cryptocurrencies and custodian wallet-service providers must now be registered under their respective Member States' competent authorities.[220] The 5th AML-directive introduced a legal definition of cryptocurrency as well as a definition of a 'custodian wallet provider'.[221] The 5th AML-directive further extends the scope of obliged entities to include virtual currency platforms and custodian wallet providers, which were not subject to the AML-regime previously.[222] Moreover, persons trading or acting as intermediaries in the trade of art, including when it is carried out by art galleries and auction houses become obliged entities when the transaction amounts to €10,000 or more.[223] In other words, these service providers now have to conduct customer due diligence, regular risk assessments, monitor and report suspicious activities.

Aside from requiring registration and customer due diligence for cryptocurrency service providers, the 5th AML-directive also mandated for FIUs to obtain addresses and identities of virtual currency-owners, which is a step to tackle the anonymity associated with virtual currencies.[224] Another step taken to increase transparency is through stipulating a prohibition against anonymous accounts, anonymous passbooks, or anonymous safe-deposit boxes.[225] Similarly, for the increased transparency in transactions initiated through the internet, the threshold prompting customer identification has been lowered from €100 to €50.[226]

---

[217] ibid, Article 32(1).
[218] ibid, Article 32(3) 4th AML; The Action Plan (n 164) 8.
[219] Council Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 'amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU' [2018] OJ L 156, Recital 8 of the 5th AML-directive. Hereinafter 'the 5th AML-directive'.
[220] ibid, Article 47(1).
[221] Article 1(d) of the 5th AML-directive. 'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically; "Custodian wallet provider" means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.
[222] ibid, Recital 8.
[223] ibid, Article 1(i).
[224] ibid, Recital 9.
[225] ibid, Article 10.
[226] ibid, Recital 14 and Article 12(2). Previously €100, see Article 12(2) 4th AML.

5.5 Directive 2018/1673 (6th AML-directive) – Hardening corporate responsibility and encouraging exemplary sanctions

The 6th AML-directive is the most recent AML-Directive which was published in the Official Journal of the EU in 2018. It complements and reinforces the 4th AML-directive and lays down measures aimed to encourage financial institutions and authorities to further strengthen their efforts against money laundering.[227] It allows Member States to introduce measures that criminalise offenders who suspect or ought to have known that the property came from a criminal activity.[228] The 6th AML-directive also focuses on predicate crimes and methods of illegal acquisition of goods and money, which may aid financial institutions and financial authorities in identifying the steps involved in complex money laundering-schemes.[229] Additionally, the provided definitions of predicate offences for money laundering are meant to facilitate uniformity to ensure that the offences are punishable in all Member States, which prevents the exploitation of more lenient jurisdictions.[230]

Furthermore, the 6th AML-directive imposes a tougher punishment where corporate responsibility is included in the fight against money laundering. For instance, in a situation of flawed supervision where a person in leadership position enabled the criminal act, Article 7 of 6th AML-directive imposes liability on legal persons. Moreover, Article 8(a)-(f) of 6th AML-directive lists criminal and non-criminal fines alongside other sanctions on legal persons. These include the denial of government benefits, restriction of commercial activities, imposition of judicial surveillance, temporary or permanent closure of establishments. For criminal punishments, responsible professionals may be imprisoned. It is thus evident that natural persons may be sanctioned under the 6th AML-directive.[231]

Prior to the 6th AML-directive, the AML-regime only targeted those who directly benefit from money laundering. The rules introduced in this directive also hold the "enablers" of money laundering and terrorist financing legally liable. The scope of penalties for money laundering-crimes is thus extended in Article 4 of 6th AML-directive, where punishment can be imposed for aiding, abetting, inciting, and attempting a money laundering offence. It further lays down a possibility for Member States to impose criminal, administrative or other types of sanctions such as the exclusion from public benefits, temporary or permanent disqualification from commercial activities or closure of the establishment which has been used for committing the offence.[232]

---

[227] Council Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 'on combating money laundering by criminal law' [2018] OJ L 284; EUR-Lex, 'Combating money laundering by criminal law' (EUR-Lex 02 Mars 2022) <https://eur-lex.europa.eu/EN/legal-content/summary/combating-money-laundering-by-criminal-law.html> Accessed 27 February 2023. The 6th AML-directive is part of the package of legislation against money laundering and terrorist financing.
[228] Article 3(2) 6th AML-directive.
[229] ibid, Recital 5, Article 2 of the 6th AML-directive.
[230] ibid, Recital 5.
[231] ibid.
[232] ibid, Article 8.

Lastly, the 6th AML-directive further strengthens the cooperation between EU Member States and includes Eurojust for assistance between the Member States when needed.[233] To summarise, the 6th AML-directive enables greater penalties for money laundering offences, emphasises liability for legal persons and natural persons and encourages authorities to impose various dissuasive sanctions.[234] It therefore hardens corporate responsibility through providing a regime which scrutinises private entities and persons for negligence and failure to comply with AML-obligations.

5.5.1 Tackling obscurities of money laundering with far-reaching obligations

In the context of preventing money laundering, these measures and obligations can enhance transparency and effectiveness in the prevention of financial crimes. Particularly, it relies on the Member States to create incentives for obliged entities to document, monitor and report suspicious activities to FIUs to prevent sanctions by public functions.[235] Against this backdrop, there is a risk that obliged entities and Member States, in order to demonstrate compliance with AML-directives, take excessive measures and in turn, compromise data protection standards.[236] The notion that far-reaching measures are applied is confirmed by the EU Commission in its Action Plan concerning the prevention of money laundering and terrorist financing.[237] Therefore, the application of far-reaching measures by different actors in the AML-regime may result in implications which negatively affects individuals in the context of fundamental rights to privacy and data protection.

6. AML-obligations and its Contentions with the Fundamental Right to Privacy

As previously stated, the AML-measures imposes obligations on private entities to perform due diligence-measures about its users to prevent money laundering and terrorist financing. The AML-Directives have also extended this obligation to conduct due diligence upon new obliged entities, including art traders.[238] As such measures involve the gathering of personal data, the retention and monitoring of data-anomalies, it can be translated into the 'processing' of personal data in the context of data privacy.[239] Since 'obliged entities' are predominantly service providers in the financial sector and certain other sectors, they are not regarded as 'competent authorities' which are allowed specific discretion to process data for the prevention, detection or investigation of crime unless they are cooperating with law enforcement which is

[233] ibid, Article 10.
[234] ibid, Recital 13.
[235] Benjamin Vogel (n 175) 53. In practice, obliged entities will create evidence to show that they complied with the AML-procedures and thus risk non-compliance with the GDPR.
[236] Nicholas James Ryder, 'Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System' (2018) 19 *German Law Journal,* 1185–1186.
[237] The Action Plan (n 164) 1-4.
[238] Article 1(i) 5th AML-directive.
[239] Article 2(1)-(2) of the GDPR.

in control of the processing.[240] Since the obliged entities under the AML-regime are not law enforcement authorities, or cooperating with competent authorities, the main framework for data protection that the obliged entities are subject to when processing data is the GDPR.[241]

6.1 Investigatory Obligations of Private Entities and Their Compatibility with Privacy Requirements

Given that obliged entities must carry out customer due diligence and submit suspicious activity reports, there may be impacts on persons whose data is being processed. For example, in a situation where a person is established in a 'high risk third country' or when there are 'doubts about the veracity and adequacy' of the information, the obliged entities must perform enhanced customer due diligence where scrutiny of the person is increased. Due to such increased scrutiny, the principles of purpose limitation and data minimisation as required in Article 5(b)-(c) GDPR is practically irreconcilable with the AML-obligations when personal data must be continuously collected to fulfil the obligations in the AML-framework. Consequently, all processed personal data might not be relevant or limited for a specified purpose.[242] Additionally, the transparency of such processing is compromised since there is a prohibition of disclosure in Article 39 of the 4th AML-directive if a suspicion of money laundering is found. In short, the rights of the data subject (the right to erasure, for example) and the obligation to facilitate the exercise of those rights are overshadowed to fulfil AML-obligations.[243]

6.1.1 Proportionality, suitability, and safeguarding privacy rights during data collection for customer due diligence

Moreover, obliged entities must consider risk factors concerning a customer's likelihood of being connected to financial crimes. This entails gathering information which could be particularly sensitive, as the obliged entity must scrutinise the individual's behaviour and character to determine whether that person, or a relative of that person is a PEP, whether any of them is established in a high-risk third country or has *connection* to a high-risk sector. It is unclear what degree of connection to a high-risk sector would prompt an enhanced due diligence-scrutiny on a customer. Nevertheless, considering that the obliged entities lack expertise and experience in detecting criminal activities, there is a great chance that excessive information is gathered about an individual in the sense that it needs to comply with the AML-obligations to avoid sanctions, thereby neglecting its GDPR-duties.[244] An example of such risk manifests when the obliged entities document information from media reports or other sources of information, such as criminal records or allegations of crimes, where there is a likelihood

[240] Article 2(2)(b) of the GDPR refers to the LED which is the data-processing directive for 'competent authorities' (law enforcement authorities); Recital 19 of the GDPR. The LED includes private entities as 'competent authorities' to process data for criminal-related purposes when they are cooperating with law enforcement.
[241] Article 2(1) and 2(d) of the GDPR.
[242] ibid, Recital 39 and Article 5.
[243] ibid, Article 12(2).
[244] The AMLD and the ECJs jurisdiction on data retention, 52.

that special categories of data are processed.[245] Following such processing of special categories of data, Article 9 GDPR requires an explicit consent from the person whose data is being processed. In addition to an explicit consent, the obliged entity must give one or more specified purposes to process a person's sensitive data.[246]

Understandably, waiting for a customer's consent to scrutinise their sensitive data could undermine the effectiveness of customer due diligence measures.[247] However, to lawfully process sensitive data in accordance with the GDPR, it is required by Article 9(g) GDPR that the processing of special categories of data must be *necessary* for reasons of substantial public interest. It must be based on EU or Member State law, but more importantly, it must be *proportionate* to the aim pursued and respect the essence of the right to data protection while also providing *suitable and specific safeguard* to the fundamental rights and the interests of the data subject.[248] If the Member State is unable to safeguard these conditions, permitting obliged entities to process sensitive data risks violation of the GDPR and the principles laid out in Articles 7 and 8 of the EU Charter. This situation is similar to the reasoning laid out in cases *Schrems* and *Tele2 Sverige*, where the CJEU ruled that allowing for an *indiscriminate* retention of metadata is a serious interference of the fundamental right to privacy.[249] Therefore, only the objective of fighting *serious crimes* could justify the retention of such data. In addition, measures must be based on objective evidence that there is a link, at least an indirect link, to serious criminal offences.[250] It is unclear whether *allegations* of criminality or terrorism would suffice as an indirect link to a serious offence which permits intrusion to the right to privacy.[251]

6.1.2 Risks of legal consequences and repressive measures for persons using financial services

Moreover, the conferral of quasi-investigatory tasks to the obliged entities to process, gather and exchange information with other obliged entities about individuals is likely to be considered as large-scale processing operations under the GDPR.[252] This matter is addressed in Recital 43 of the 4th AML-Directive, where the collection and processing of personal data by obliged entities must be 'limited to what is necessary for complying with the AML-obligations and should not be processed further'.[253] However, in the light of the GDPR, such operations could bear implications for the rights and freedoms of the persons, particularly if those operations create difficulties for the individuals to exercise their privacy rights.[254] Where personal aspects (behavioural information, for example) are processed, an impact assessment is required by the GDPR, due to the sensitivity of such information. An impact assessment is

[245] Article 9(1) of the GDPR.
[246] Recital 51 GDPR.
[247] Recital 46 of the 4th AML-directive. This Recital addresses the risk of undermining the effectiveness of the fight against money laundering and terrorist financing if the customer could access their data.
[248] Article 9(g) GDPR.
[249] *Tele2 Sverige* (n 80) paras 99-100; Maja Brkan (n 101) 873.
[250] ibid, 111.
[251] The EBA Guidelines (n 195) 28. It is encouraged to document allegations of crime as part of the risk assessment.
[252] Recital 91 GDPR.
[253] Recital 43 of 4th AML-directive.
[254] Recital 91 GDPR.

significant where such collection of data could prevent an individual from exercising a right or using a service or contract, such as in the case of financial service providers exercising investigatory powers.[255] Since obliged entities must process personal aspects and can, on the basis of their findings, blacklist persons from using financial services while being under the prohibition of disclosure, there are significant difficulties for persons to exercise their data-protection rights. For this reason, the GDPR requires such impact assessment before data-gathering obligations are carried out under the AML-frameworks.[256]

6.1.3 Exchange of information between obliged entities

When an obliged entity deems that there is a suspicious transaction, they are entitled to share that information with other obliged entities, even where the suspicious transaction has never been verified by an FIU or public authority.[257] This may escalate proportionality concerns as individuals may be subjected to categorisations, repressive measures, or stigmatisation in commercial activities.[258] Consequently, such measures risk negative impacts on the financial security of the persons affected if they are blacklisted from accessing their accounts based on suspicions detected by the obliged entity.[259]

Although financial information and suspicious activity reports have been a part of the financial sector for a long time as part of banking-duties in accordance with other legal frameworks, it is important to note that the AML-regime consists of *investigatory tasks* which relies on private entities, rather than rules solely for retention and record-keeping.[260] It therefore diverges from the traditional approach to investigations and data-collection to detect criminal activities entrusted to law-enforcement authorities. Without adequate safeguards to privacy laid down by the Member States to balance the repressive nature of the AML-duties, personal information processed between obliged entities and the public authorities (or an FIU) creates a risk that privacy protection becomes overshadowed due to the intrusive and repressive measures employed to detect financial crimes and terrorist financing.[261]

6.2 Lack of Data-processing Restrictions of Financial Intelligence Units

In the context of privacy rights, FIUs operate with significant investigatory powers conferred to them by the AML-regime. These investigative powers include the exchange of relevant

[255] Recital 91 GDPR.
[256] ibid. Large-scale processing affects a large number of persons and is likely to result in a high risk.
[257] Article 39(5) of the 4th AML-directive.
[258] Benjamin Vogel (n 175) 57.
[259] Article 14(4) of the 4th AML-directive stipulates that transactions must be stopped and the business relationship terminated upon detection of suspicious activity.
[260] Lukas Martin Landerer, 'The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention, A Flawed Comparison?' [2022] The European Criminal Law Associations' Forum, 'The Prevention and Fight against Money Laundering – New Trends' 1st edition <https://eucrim.eu/issues/2022-01/> Accessed 22 May 2023, 68-71. Financial data retention and record-keeping has been a part of the normal tasks and functioning of financial institutions as required by other legal frameworks on both EU and national level.
[261] Benjamin Vogel (n 175) 57; EDPB Statement (n 9) 1-2. The EDPB highlights data-protection challenges related to AML in the past and expresses the need to address the interplay between privacy protection and AML-measures.

information between FIUs to process and analyse data concerning financial crimes or terrorist financing, as well as cooperation 'to the greatest extent possible'.[262] It therefore seems like the exchange of personal data between EU FIUs is only allowed for the purpose of analysing that information and that the data should not be used for an investigation or prosecution, unless the requesting FIU obtains a prior consent from the data-sharing FIU.[263] However, for certain FIUs, the line between analysis and investigation is unclear.[264] This directly undermines the principle of purpose limitation stipulated in Article 5 of the GDPR, since the very purpose could be to either *investigate*, or analyse, both of which are inherently broad in nature.[265]

The general rule for all measures carried out in the scope of EU law must be in accordance with the fundamental rights and not undermine the primacy, effectiveness, and unity of EU law.[266] The same applies to investigative activities.[267] Article 33 of the 4th AML-directive stipulates that obliged entities must respond and exchange information about *any* suspicious activities to FIUs to fulfil their obligations. The FIUs may then analyse the information to establish links between suspicious transactions and criminal activity. Upon suspicion of predicate offences to money laundering or terrorist financing, the FIU sends its findings in a report to law enforcement authorities.[268] Law enforcement authorities may also request information directly from obliged entities.[269] Despite the legal emphasis on the compliance with fundamental rights, there is a risk that a public-private partnership could lead to the gathering of information for criminal proceedings rather than strictly being limited to investigation by the FIU. Regarding such risk for purpose limitation, the EU Commission expresses that Member States should regulate the exchange of personal data to ensure compliance with its procedural rules.[270] However, it is unclear whether the AML-frameworks provide sufficiently clear and precise safeguards for Member States to adequately observe Articles 7 and 8 of the EU Charter and its conditions.

6.2.1 FIUs and legal uncertainties: between the GDPR and the LED for investigations and criminal proceedings

As previously stated, the characteristics of FIUs vary across the EU.[271] This creates uncertainty concerning which data protection framework the FIUs are governed by. Interestingly, Article 32(1) of the 4th AML-directive stipulates that the prevention and detection of criminal offences is a core responsibility of FIUs.[272] Despite the clarity of the core tasks, Article 41 of the 4th AML-directive stipulates that the applicable framework governing FIUs is the Data Protection

[262] Article 53(1) 4th AML-directive, amended by the 5th AML-directive.
[263] Foivi Mouzakiti (n 213) 357.
[264] ibid.
[265] ibid.
[266] Melloni (n 58) para 67.
[267] Commission, 'On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing' [2022] SWD(2022) 347 final, 16.
[268] Article 32 of the 4th AML-directive.
[269] SWD(2022) 347 final (n 267) 2.
[270] ibid, 17.
[271] Foivi Mouzakiti (n 213) Some FIUs are organisationally administrative, some as part of police enforcement, some are hybrid in organisational structure.
[272] ibid, 365.

Directive (the GDPR's predecessor).[273] It is then clarified in the 4th AML-directive that it is 'without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters'.[274] This means that FIUs could either be governed by the GDPR, but also by the LED which does not require transparency in the processing of personal data, while also granting broader discretion for data-processing and fewer data protection rights for individuals.[275]

Furthermore, due to the cross-border nature of financial crimes, FIUs must share suspicious reports with another Member State even in the absence of a specific request. For example, when a FIU receives a report about a suspicious transaction relevant to another Member State, the receiving FIU is obliged to promptly share it with that Member State.[276] Article 53(2) of the 4th AML-Directive also stipulates that a FIU which receives a request from another EU FIU, must employ the 'whole range of powers' that are available to them.[277] This 'whole range of powers' conferred upon the FIU enables it to request national banks to request data concerning a person's financial records among other data. FIU may also consult *any* databases which are not part of the AML-framework (non-obliged entities).[278] The range of sources and data a domestic FIU may activate and have access to on behalf of its EU counterparts is thus broad, potentially functioning as a gateway to access *indiscriminate* sources of information.[279] This uncertainty concerning the applicable framework has been noted by the EU Commission, which confirms that there is an uneven application of EU data protection rules where safeguards, security and confidentiality vary across Member States.[280]

The request itself contains the background information, facts, reasons for the request, and how the information will be used.[281] While some FIUs require the request to be 'adequately motivated' to share data, some do not require such justifications. In the light of *Digital Rights,* extensive retention of data without clear and precise rules to limit the extent of interference in a person's privacy is considered by the CJEU to be a serious interference with Article 7 and 8 of the EU Charter.[282] Aside from the issue of blurred purposes in the FIU requests, it is also difficult for a FIU to refuse data-sharing. Article 53(3) of the 4th AML-directive stipulates that a FIU may only refuse to exchange information in *exceptional* circumstances where the exchange would violate fundamental principles of its national law. Seemingly, free exchange of requested data is favoured over the limitations of such.[283]

[273] Recital 42 of the 4th AML-directive.
[274] ibid; Mouzakiti (n 213) 363-364. The Commission confirmed the viewpoint that FIUs shall fall under the GDPR, as they are considered a 'public administration'.
[275] Nadezhda Purtova (n 131) 60-61; Recital 12 of the LED.
[276] Article 53(1) 4th AML-directive.
[277] Article 53(2) 4th AML-directive.
[278] No restriction of which information sources a FIU may request access to is stated in the AML-directives.
[279] Mouzakiti (n 213) 358.
[280] Commission staff working document 'On improving cooperation between eu financial intelligence units' 26.6.2017 SWD (2017) 275 final, 6.
[281] Article 53(1) 4th AML-directive.
[282] Digital rights (n 84) paras 66-69. Mutual trust principle could however hinder FIUs from questioning the validity of requests to share data from other Member States.
[283] Foivi Mouzakiti (n 210) 359.

6.3 Data Protection Flaws of the Proposed AML-regulation

When it comes to the proposal for an AML-regulation, the European Data Protection Board (EDPB) raised serious doubts concerning the compatibility of the provisions proposed by the Council. In a Letter by the EDPB,[284] AML-measures in the proposed regulation are considered to impose broad and far-reaching obligations on obliged entities for the identification, monitoring and reporting of their customers, essentially affecting *all persons* using financial services.[285] This analysis draws attention to the CJEU's judgement in *Digital Rights*, where personal data was gathered without limitation of scope and time and carried out without prior warranty, was deemed an interference with Article 7 and 8 of the EU Charter.[286]

Furthermore, the EDPB addresses risks connected to the lawfulness, necessity and proportionality of the AML-measures as follows. First, the cooperation between private and public authorities allows the obliged entities to monitor its customers on behalf of law enforcement authorities, possibly with connection to ongoing criminal investigations. This, according to the EDPB, 'would entail significant risks from a data protection perspective'.[287] Second, the EDPB criticises that the provisions proposed by the Council allows data-exchanges between obliged entities without the scrutiny from public authorities. This data exchange between obliged entities is meant to be used for due diligence measures. In the view of the EDPB, the possibility for obliged entities to exchange personal data about its customers implies a broad processing of data, resulting in mass surveillance by private entities. For this reason, the proportionality of the measure is questioned.[288]

Third, the EDPB states that depending on the information gathered about a customer, an obliged entity can terminate or restrict its financial services to a customer who is deemed suspicious of money laundering or terrorist financing. Known as 'de-risking', this practice could lead to financial insecurity as the account is restricted or difficulties arise when opening a new account.[289] If the proposed regulation is adopted without consideration to the flaws in

[284] The EDPB is an independent body in the EU which is established by the GDPR. It promotes cooperation between data protection authorities in the EU and encourages consistent application of data protection rules across the EU. See <https://edpb.europa.eu/concernant-le-cepd/concernant-le-cepd/who-we-are_en> Accessed 19 April 2023.
[285] European Data Protection Board, 'EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations' [2023] <https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-european-parliament-council-and-european_en> Accessed 25 May 2023. 5 Hereinafter 'EDPB Letter 2023'; Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing' [2021] COM(2021) 420 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420> Accessed 1 May 2023.
[286] *Digital Rights* (n 84) para 65.
[287] EDPB Letter 2023 (n 285) 3; European Data Protection Supervisor, 'on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing' [2020] Opinion 5/2020. <https://edps.europa.eu/sites/edp/files/ publication/20-07-23_edps_aml_opinion_en.pdf.> Accessed 1 May 2023, para 43. The European Data Protection Supervisor (EDPS) is an independent supervisory authority which monitors EU institutions and bodies' compliance with the right to privacy and data protection.
[288] EDPB Letter 2023 (n 285) 3.
[289] Council of Europe, 'De-risking' (www.coe.int) <https://www.coe.int/en/web/moneyval/implementation/de-risking> Accessed 21 April 2023.

privacy protection, the EDPB expresses that there would be serious doubts regarding the compatibility of the AML-regulation with data-protection rights.[290]

7. Conclusion

To answer the first research question whether the AML-Directives require private entities and FIUs to scrutinise individuals in a way which risks violation of privacy rights, it is evident that private entities must gather personal information in a far-reaching manner which risks incompliance with a robust privacy framework. Despite fundamental rights cases clarifying the prohibition of interference with the right to privacy and personal data, the AML-directives and the proposed regulation largely rely on the private sector to gather, monitor, and detect risks. Such processing also entails the analysis of a person's behaviour to determine ties or risk of ties to financial and terrorist crimes, thereby granting private entities discretion to process personal data in a manner which could violate the principles established under privacy rights. Such rights, also concretised in the GDPR, require the purposes for data-processing to be specific and explicit and determined at the time of the collection. The information collected must be relevant for that specified purpose and limited to what is necessary to achieve it. In particular, the rights of the data subject must be ensured under the GDPR. It is however questionable how the individual's right to access, rectify, erasure and transparency can be exercised in the context of the AML-directives where there is a prohibition of disclosure. While banks have historically been subject to obligations requiring documentation of their customers' funds, the AML-directives are directly requiring scrutiny of personal data for the sole purpose of detecting financial crimes, a task typically belonging to law-enforcement entities.

The scope of entities which are obliged to fulfil the AML-framework has expanded to include not only service providers from the financial sector, but also Fintech, and other sectors. This means that private entities with no expertise or experience about investigations, data analysis and lawful processing of data are required to gather information about *all individuals* using financial services for the purpose of detecting crimes or relationships with a PEP. The lack of expertise about data-protection principles and financial crimes creates a risk of excessive monitoring, consequently risking violation of the GDPR where purpose-limitation, data-minimisation and proportionality is required when processing sensitive data. As a person's transactions, use of services and media-information is processed, such data allows for very precise conclusions to be drawn concerning a person's habits, activities, and social environment. Should the Member States fail to incorporate privacy protection in their implementation of the AML-Directives, the interference of personal data would be particularly serious as negative effects could impact individual's financial security, reputation, and lead to investigations with legal implications. Additionally, case *Tele2 Sverige* requires (at least) an indirect link to serious crimes for the FIU to access data retained without specified purpose and limitations. Considering that obliged entities, depending on which sector they belong to, lacks expertise in detecting crimes, it is questionable whether a suspicion of crime based on private entities' observation provides a sufficient link to serious crime which allows the FIU to exercise its intrusive powers to process data without violating Article 7 and 8 of the EU Charter.

[290] EDPB Letter 2023 (n 285) 3.

To answer the second research question, the conflicts between the AML-obligations and EU privacy rights are as follows.

Obliged entities' obligations to gather personal information

The collection of data, risk-assessments and monitoring suspicious activities for purposes related to criminality has traditionally been the task of the law enforcement-entities. As stated above, the lack of expertise contributes to greater risk of flawed data protection-procedures or arbitrary application of repressive measures. In the context of the GDPR, the obliged entities are still regarded as data processors which are not part of 'competent authorities' entrusted with public functions. As the private entities are not competent authorities, there is no discretion to process data for the prevention, detection, or investigation of crime in accordance with the LED. Although some provisions in the AML-framework mention the importance of data-protection, it is questionable whether such statements are effective since the nature of AML-obligations entails continuous scrutiny of an individual without specificity, purpose limitation, threshold of suspicion or prior warranty.

Financial intelligence units and their indiscriminate access to data

Another way which a Member State's implementation of the AML-directives could violate privacy rights can be seen in the AML-directives conferral of investigative powers to the FIUs. In the AML-Directives, the FIUs are granted broad data-processing powers and investigative powers. Despite such permissiveness, there are no explicitly mentioned limitations about data-processing-powers of the FIUs, meaning that thresholds, scope, and limitations are not laid out in the AML-directives. In other words, the AML-regime does not include provisions to limit the extent of interference to Articles 7 and 8 of the EU Charter. Therefore, the protection of privacy when implementing AML-measures is solely reliant on the Member States, where some will not be able to adequately fulfil the conditions of 'clear, precise with adequate safeguards' as stipulated in *Digital Rights* when conferring the AML-powers of the FIUs.

Moreover, FIUs must cooperate to the greatest extent possible while also employ the whole range of powers available to FIUs. This means that the FIU which receives a request to share data from another Member State's FIU, must use *all* sources of information they can access to exchange that information. It therefore functions as a gateway for other Member State's FIUs to gain access to unlimited information-sources. Furthermore, FIUs may access individuals' financial records and non-financial information from databases which do not belong to the financial sector, thereby being unrestricted in what type of information they may collect and exchange to another Member States' FIU. Even if a Member State introduces limitations to FIUs discretion to exchange personal data, Article 53(3) of the 4th AML-directive makes it difficult to refuse data-sharing by requiring *exceptional circumstances* for the refusal to exchange information to another Member State's FIU. A Member State also risks breaching the principle of mutual trust by refusing to exchange personal data, even if the refusal is for the protection of privacy.

Additionally, there is uncertainty regarding *which* data protection-framework an FIU is subject to, as some are subject to the GDPR, being the restrictive data protection-framework, while some FIUs are subject to the broad discretion-enabling LED. This uncertainty makes data protection-measures difficult for Member States to uphold, since other Member State's FIU may operate under differing protective standards.

Fundamental rights implications

Despite the emphasis of the right to privacy and data protection in *Digital Rights* and *Tele2 Sverige*, there is a complexity concerning the application of the GDPR and the protection of privacy when Member States are fulfilling AML-obligations. On the one hand, Member States may introduce more intrusive measures to tackle financial crimes. On the other hand, individuals are afforded a strong protection of privacy rights in Article 7 and 8 of the EU Charter. In the light of case *Digital Rights,* the Data Retention Directive was annulled precisely due to the extensive retention of data without clear and precise rules to limit the extent of interference in a persons' fundamental rights under Articles 7 and 8 of the EU Charter. It is clarified that extensive retention of data cannot be carried out without the safeguard of clear and precise rules to limit the extent of interference in a person's privacy.

Furthermore, as Member States are allowed to introduce stricter monitoring of individuals, there is a risk of violation of the safeguarding conditions for data retention in cases *Schrems* and *Tele2 Sverige*. In those cases, it was established by the CJEU that the retention of data about individuals is an interference with the essence of privacy if the data are stored without differentiation, limitations or exceptions for the objectives pursued. As stated above, AML-measures entails an ever-changing monitoring of individuals where data about relatives, associated sectors and even information from media must be analysed and documented by the obliged entities – measures which raises serious doubts about the compatibility with privacy norms as expressed by the EDPB. Without those safeguards, the Member States risk serious interference of Article 7 and 8 of the EU Charter.

Privacy rights overshadowed by incoherent norms

Adding to the incoherency of norms is that in case *Melloni*, the CJEU stipulates that Member States cannot apply national fundamental rights if it undermines the mutual trust and recognition between Member States. This means that a Member State cannot apply their own, stronger national privacy standard to allow a national FIU to refuse a data-exchange request from another Member State's FIU. Particularly, the Member State is not allowed to apply national laws where it interferes with EU fundamental rights, the primacy, unity, and effectiveness of EU law. However, in case *TSN*, it is shown that Member States can apply *favourable* conditions falling outside of the scope of EU law. Against this backdrop, a stronger protection of personal data may be applied by a national court insofar as it does not undermine the primacy, unity and effectiveness of EU law and is in conformity with the EU Charter. Despite such a possibility granted under Article 53(1) EU Charter, there is still a great risk of Member States undermining the primacy, unity, and effectiveness of EU law since the discrepancies between privacy and AML creates great difficulties in navigating requirements of privacy norms while upholding AML-directive.

The contingency between the AML-obligations and the privacy rights highlights an incoherency which could negatively affect Member State's ability to comply with either of the norms as they must navigate the conflicting norms. Specifically, these inconsistencies lead to great risks that Member States may not be able to fulfil their obligations in accordance with both the data protection framework and the AML-directives together.

It is noteworthy that despite the crime-fighting nature of the AML-directives, the basis for them is Article 114 TFEU. Due to the adoption of intrusive AML-measures with the legal basis for harmonisation of the internal market, the incoherent norms can be interpreted as driven by an economic approach. As the guardian of the internal market, it is understandable that the main objective of the EU is to facilitate commercial harmonisation for the elimination of barriers in the internal market. However, the application of an economic approach to principles built upon fundamental rights weakens the credibility of the EU Charter and the coherency of norms within the EU. Therefore, in the implementation of AML-directives, the interference with rights to privacy and data protection without clearly delineated safeguards for Member States to establish, risks violating the principles of necessity and proportionality as required in Article 52(1) of the EU Charter. The practical effects of these discrepancies could potentially erode the significance of privacy rights established under Articles 7 and 8 of the EU Charter, leading to an underprioritised and inadequate protection of privacy where a mass surveillance by private entities is permitted under the guise of financial integrity.

8. Bibliography

Case law

Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:627, Opinion of AG Bot

Case C-311/18 - Facebook Ireland and Schrems (Schrems) [2020] ECLI:EU:C:2019:1145

C-203/15 Tele2 Sverige [2016] ECLI:EU:C:2016:970

Joined Cases C-293/12 and C-594/12 Digital Rights [2014] ECLI:EU:C:2014:238

Klass and Others v Germany, App no 5029/71 (ECtHR 6 September 1978)

Malone v UK, App no 8691/79 (ECtHR 2 August 1984)

Case C-2/92 Bostock [1994] ECLI:EU:C:1994:116

Case 5/88 Wachauf [1989] ECR 2609

Case C-260/89 ERT [1991] ECLI:EU:C:1991:254

Case C-309/96 Annibaldi [1997] ECLI:EU:C:1997:631

Case C-8/74 Procureur du Roi v Benoît and Gustave Dassonville [1974] ECLI:EU:C:1974:82

Case C-601/15 J. N. v Staatssecretaris van Veiligheid en Justitie [2016] EU:C2016:84

Case C-131/12 Google Spain [2014] ECLI:EU:C:2014:317

Case C-136/17 GC and Others v Commission nationale de l'informatique et des libertés [2019] ECLI:EU:C:2019:773

Case C-144/04 Mangold [2005] ECLI:EU:C:2005:709

Case C-555/07 Kücükdeveci [2010] ECLI:EU:C:2010:21

Case C-617/10 Åklagaren v Hans Åkerberg Fransson [2013] ECLI:EU:C:2013:105

Case C-112/00 Schmidberger v Austria [2003] ECLI:EU:C:2003:333

Case 11-70 Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel [1970] ECLI:EU:C:1970:114

Case no 1-58 Friedrich Stork & Cie v High Authority of the European Coal and Steel Community [1959] ECLI:EU:C:1959:4

Case 4-73 J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities [1974] ECLI:EU:C:1974:51

Case C-399/11 Melloni [2013] ECLI:EU:C:2013:107

C-609/17 – TSN [2019] ECLI:EU:C:2019:981

Case 43-75 Defrenne [1976] ECLI identifier: ECLI:EU:C:1976:56

Legal frameworks

Consolidated Version of the Treaty establishing the European Community [2000] OJ C 325

Council Directive (EU) 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105

Council Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May [2015] on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141

Council Directive (EU) 2016/680 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 [2016] OJ L 119

Council Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 ‘on combating money laundering by criminal law’ [2018] OJ L 284

Council Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ’amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU’ [2018] OJ L 156

Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol’s cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol’s role in research and innovation [2022] OJ L 169

United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III). <https://www.ohchr.org/en/human-rights/universal-declaration/translations/english> Accessed 31 March 2023

Official publications

Commission, ‘Fight against money laundering and terrorist financing: Commission assesses risks and calls for better implementation of the rules’ (www.ec.europa.eu, 24 July 2019)

<https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452> Accessed 18 February 2023

Commission, 'on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' [2012] COM/2012/0168 final

Commission, 'on the EU Strategy to tackle Organised Crime 2021-2025' (2021) COM(2021) 170 final

Commission, 'On the protection of individuals in relation to the processing of personal data in the Community and information security' COM (90) 314 final

Commission, 'On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing' [2022] SWD(2022) 347 final

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing' [2021] COM(2021) 420 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420> Accessed 1 May 2023

Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010 [2021] COM (2021) 421 final

Commission, 'on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' (2020) 2020/C 164/06

Commission, 'on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities' (Commission staff working document – Accompanying the document report from the commission to the European Parliament and the Council) (2022) SWD (2022) 344 final

Commission, 'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework' (2019) COM (2019) 360 final

Commission, 'Upgrading the Single Market: more opportunities for people and business' (Communication) COM (2015) 550 final

European Banking Authority 'Guidelines on on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849' [2021] EBA/GL/2021/02

European Data Protection Board, 'EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations' [2023] <https://edpb.europa.eu/our-work-tools/our-

documents/letters/edpb-letter-european-parliament-council-and-european_en> Accessed 25 May 2023

European Data Protection Supervisor, 'on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing' [2020] Opinion 5/2020. <https://edps.europa.eu/sites/edp/files/ publication/20-07-23_edps_aml_opinion_en.pdf.> Accessed 1 May 2023
European Parliament, Council of the European Union, European Commission, 'Explanations relating to the Charter of Fundamental Rights' [2007] O.J C 303

Opinion 2/13 pursuant to Article 218(11) TFEU, Draft international agreement, Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Compatibility of the draft agreement with the EU and FEU Treaties, ECLI:EU:C:2014:2454

Opinion 2/13 pursuant to Article 218(11) TFEU, ECLI:EU:C:2014:2454, European Union: Court of Justice of the European Union, 18 December 2014

Opinion 2/94 pursuant to Article 228 of the EC Treaty, Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms, ECLI:EU:C:1996:140

Opinion 2/94 pursuant to Article 228 of the EC Treaty, Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms, ECLI:EU:C:1996:140, 28 March 1996

The European Data Protection Board, 'Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing' [2020] <https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_en> Accessed 25 May 2023

Journal Articles

Brkan M, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864

Groussot X, Lock T and Pech L, 'EU Accession to the European Convention on Human rights: a Legal Assessment of the Draft Accession Agreement of 14th October 2011' (2011) Fondation Robert Schuman, European Issues N°218

Koster H, 'Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework' (2020) Vol 23. 2 Journal of Money Laundering Control 379<https://www.emerald.com/insight/content/doi/10.1108/JMLC-09-2019-0073/full/pdf?title=towards-better-implementation-of-the-european-unions-anti-money-laundering-and-countering-the-financing-of-terrorism-framework> Accessed 22 May 2023

Landerer L M, 'The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention, A Flawed Comparison?' [2022] The European Criminal Law Associations'

Forum, ‘The Prevention and Fight against Money Laundering – New Trends’ 1st edition <https://eucrim.eu/issues/2022-01/> Accessed 22 May 2023

Loideain NN ’EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era’ 54 in James Schwoch, John Laprise and Ivory Mills, Surveillance: Critical Analysis and Current Challenges, Media and Communication (2015) vol 3, 53

Mouzakiti F, ’Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive’ (2020) Vol. 11(3) NJECL 351

Paunovic N, 'Terrorist Financing as the Associated Predicate Offence of Money Laundering in the Context of the New EU Criminal Law Framework for the Protection of the Financial System' (2019) 3 ECLIC 659

Pelkmans J, ’The New Approach to Technical Harmonization and Standardization’ (1987) 25 JCMS 249

Purtova N ‘Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships’ (2018) Vol. 8 International Data Privacy Law 52

Ryder N J, ’Is It Time to Reform the Counter-terrorist Financing Reporting Obligations? On the EU and the UK System’ (2018) 19 German Law Journal, 1185–1186

Vogel B, ‘Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing’ [2022] The European Criminal Law Associations’ Forum, ‘The Prevention and Fight against Money Laundering – New Trends’ 1st edition <https://eucrim.eu/issues/2022-01/> Accessed 22 May 2023

Literature

Barak A, *Proportionality: Constitutional Rights and Their Limitations* (1st edition, Cambridge University Press 2012)

Barnard C, *The Substantive Law of the EU, The Four freedoms* (6th edition OUP 2019)

Craig P and de Búrca G, *EU Law, Text, Cases, and Materials* (6th edition OUP 2015)

Craig P, ‘The Evolution of the Single Market’ in Catherine Barnard, and Joane Scott (eds), *The Law of the Single European Market: Unpacking the premises* (Bloomsbury Publishing Plc 2002)

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16 (Springer Science & Business, 2014)

Klamberg M, ’Skydd enligt Europakonventionen om skydd för de mänskliga rättigheterna’ in Cecilia Magnusson (ed), *Rättsinformatik* (Studentlitteratur AB 2016)

Reichel J, ’EU-rättslig metod’ in Nääv M & Zamboni M (red.), *Juridisk metodlära,* (2nd Studentlitteratur AB, Lund, 2018)

Schütze R, *European Union Law* (2nd edition, Cambridge University Press 2018)

Trzaskowski J and Gersvan Sörensen M, *GDPR Compliance – Understanding the General Data Protection Regulation* (Ex Tuto Publishing A/S 2019)

Tzanou M, *The Fundamental Right to Data Protection, Normative Value in the Context of Counter-terrorism Surveillance* (Hart Publishing 2017)

Egan M, ‘Single Market’ in Jones E (ed.) et al, *The Oxford Handbook of the European Union* (OUP 2012)

Reports

Europol Financial Intelligence Group,‘From suspicion to action, converting financial intelligence into greater operational impact’ (2017) Publications Office of the European Union <https://www.europol.europa.eu/publications-events/publications/suspicion-to-action-converting-financial-intelligence-greater-operational-impact> Accessed 16 February 2023

Europol, ‘Enterprising criminals, Europe’s fight against the global networks of financial and economic crime’ (2020) Europol <https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime> Accessed 21 May 2023

Europol, ‘Serious and Organised Crime Threat Assessment, a Corrupting Influence: the Infiltration and Undermining of Europe’s Economy and Society by Organised Crime (2021) Europol <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021> Accessed 21 May 2023

Europol, ‘Terrorism Situation and Trend Report’ (2022) Europol <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat> Accessed 21 May 2023

Electronic Sources

Commission, ‘Anti-money laundering and countering the financing of terrorism legislative package’ (finance.ec.europa.eu 2021) < https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en> Accessed 21 April 2023

Commission, ‘EU context of anti-money laundering and countering the financing of terrorism’ (www.finance.ec.europa.eu) <https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en> Accessed 18 February 2023

Commission, ’Questions and Answers - Commission steps up fight against money laundering and terrorist financing’ (www.ec.europa.eu, 7 May 2020)

<https://ec.europa.eu/commission/presscorner/detail/eng/qanda_20_821> Accessed 18 February 2023

Council of Europe, 'De-risking' (www.coe.int) <https://www.coe.int/en/web/moneyval/implementation/de-risking> Accessed 21 April 2023

EUR-Lex, 'Combating money laundering by criminal law' (EUR-Lex 02 Mars 2022) <https://eur-lex.europa.eu/EN/legal-content/summary/combating-money-laundering-by-criminal-law.html> Accessed 27 February 2023

European Employment Lawyers Association, 'ECJ 19 November 2019, joined cases C-609/17 and C-610/17 (TSN), Paid leave' <https://eela.eelc-updates.com/summary/eelc-2019-317545> Accessed 18 March 2023

FATF, 'History of the FATF', https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html Accessed 18 February 2023

FATF, 'Financial Action Task Force – 30 years', (www.fatf-gafi.org 2019) <www.fatf-gafi.org/publications/fatfgeneraldocuments/FATF-30.html> Accessed 18 February 2023

G7, (www.g7germany.de 2023) <https://www.g7germany.de/g7-en/g7-summit/g7-members> Accessed 18 February 2023