INTERNATIONAL
HELLENIC
UNIVERSITY

The potential conflict between the General Data Protection Regulation (Regulation (EU) 2016/679) and the Anti-Money Laundering Directives (2015/849 & 2018/843 Directives): the obligations of the financial institutions

Magdalini Leventopoulou

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES
SCHOOL OF HUMANITIES, SOCIAL SCIENCES AND ECONOMICS

A thesis submitted for the degree of

Master of Laws (LLM) in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

January 2023
Thessaloniki – Greece

Student Name: Magdalini Leventopoulou

SID: 1104200016

Supervisor: Prof. Dr Nikoletta Kleftouri

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

January 2023

Thessaloniki - Greece

ABSTRACT

This dissertation was written as part of the LLM in the Translational and European Commercial Law at the International Hellenic University. The financial sector is heavily regulated in the European Union, and financial institutions are subject to both the General Data Protection Regulation (GDPR) and the Anti-Money Laundering Directives (AMLD) provisions. This can lead to a potential conflict between the two legal instruments, as the obligations of the financial institutions may be incompatible with each other.

The aim of the present dissertation is to analyze this potential contradiction between the GDPR and the AMLDs and the impact on financial sector. In order to achieve the main goals, the research methodology includes a review of the relevant legal provisions and a comparative analysis of the potential contradictory rules related to the requirements and obligations that must be met by the financial organizations. The identification of possible solutions to reconcile the two legal frameworks is also included among the main objectives of the dissertation. Last but not least, the examination will be conducted at the EU level, although it will also include a brief comparison with the US regime in order for a more complete picture of the two conflicting needs' regulatory treatment to be achieved.

The completion of the present work would not have been possible without the useful contribution of my supervising professor, Dr Nikoletta Kleftouri, whom I would like to express my sincere gratitude to, for her guidance and invaluable assistance throughout the whole process. I would also like to thank my friends, my parents, Panagiotis & Eleni and my person, Panos who from the very beginning of my postgraduate studies were by my side encouraging me and convincing me that everything is possible!

Keywords: General Data Protection Regulation, Anti-Money Laundering Directive, Data Processing, Financial Institutions, EU law

Magdalini Leventopoulou

30th of January 2023

CONTENTS

INTRODUCTION

The General Data Protection Regulation (2016/679) has played a significant role in protecting the personal data of individuals in the financial sector. Prior to the implementation of the GDPR, there were few consistent rules governing the collection and use of personal data by financial institutions within the EU. This lack of regulation left individuals vulnerable to having their personal data misused or mishandled, and raised concerns about the security of their financial information. The global economic crisis brought these issues to the forefront, as financial institutions faced increasing pressure to protect their customers' data in order to maintain trust and confidence in the financial system. The GDPR was introduced as a response to these concerns, and provided a comprehensive framework for the protection of personal data in the financial sector, among other areas. By establishing clear rules and obligations for financial institutions, the GDPR has helped to improve the security and privacy of individuals' financial information.

The Anti-Money Laundering Directives (2015/849 & 2018/843) have contributed significantly to the global fight against money laundering and terrorist financing. Prior to the implementation of these Directives, there were few consistent standards in place across the European Union for preventing and detecting money laundering and terrorist financing. This lack of coordination made it difficult to effectively combat these activities, and left financial institutions vulnerable to being used for illicit purposes. The global economic crisis of the late 2000s highlighted the need for more robust measures to prevent financial crimes, as these activities can undermine the stability of the financial system and damage the global economy. The implementation of the AML Directives provided a framework for financial institutions to follow in order to prevent and detect these activities, and helped to build confidence in the financial system by reducing the risk of illicit activity.

The potential conflict between the General Data Protection Regulation (GDPR) and the Anti-Money Laundering Directives (AMLDs) is a topic of growing concern within the financial sector. On the one hand, the GDPR is focused on protecting individuals' personal data, and places strict limitations on how they can be collected, used, and shared. On the other hand, the AMLDs aim to prevent money laundering and terrorist

financing by requiring financial institutions to implement certain measures, such as customer due diligence and reporting suspicious activity. While these two frameworks have different goals, they can sometimes be at odds with one another, creating challenges for financial institutions in meeting their obligations under both. For example, the GDPR requires that personal data be collected and processed only for specific, explicit, and legitimate purposes, while the AMLDs require financial institutions to collect and process a wide range of personal data by their customers, under the KYC requirements in order to identify and prevent money laundering and terrorist financing.

This essay will examine the potential conflict between the GDPR and AMLDs in the context of the obligations of financial institutions. By examining the requirements and the main provisions of both legislations, and the challenges that financial institutions face in meeting their requirements, we can gain a better understanding of the potential conflict between these two regimes and the impact it may have on the financial sector. Additionally, we will consider potential solutions to this conflict, and the role that financial institutions can play in ensuring compliance with both regulatory frameworks. In order to provide context for this discussion, we will also consider the background and purpose of the regulatory schemes, as well as the current state of the financial sector and the specific challenges it faces in complying with both the GDPR and AMLDs.

1. EU GENERAL DATA PROTECTION REGULATION

As already mentioned at the above introduction, the main goal of the present dissertation is to examine the correlation of two of the most important legal instruments that affect the financial sector and shape its regulatory regime. Nevertheless, before we focus on the specific legal issues that arise from the potential contradiction between the two pieces of legislation, an overview of both the respective legal texts and in particular the rules provided for the financial institutions, is essential. In chapter 1, an analysis of the EU General Data Protection Regulation and its main provisions will be conducted.

1.1. Historical Background

Data is all around us: our name, a simple picture of us, our age, our gender, our contact details. Each human entity is associated with a large number of data which ultimately constitute the characteristics that differentiate one entity from another and make each of them unique.

In our daily life, our personal data are requested everywhere, for a transaction with the bank, a purchase via the internet - and not only -, our access to a website, our participation to a survey etc. Undoubtedly the majority of the cases which require our personal data are through technological means. The consequence of this is the fact that the rapid development of technology and the absolute protection of the data subjects are two inversely proportional concepts: the more the former develops, the more are the risks that poses for its users. In what way are the data of those technologies' users take place? Are they transferred elsewhere? Is the processing of the data lawful? And in the end, to what extent are the subjects' data, and therefore the subjects themselves, protected?

The above constitute only an indicative list of the issues that made the adoption of a harmonized legal regime within the EU imperative, in order to ensure the safe movement of the data of the European citizens and to set the foundations, limits and legal bases for the data reasonable and lawful processing.

The first attempt of the European legislators to adopt a data protection-related set of rules was the Data Protection Directive 95/46/EC[1] which was enacted on the 24th of October 1995 and came into force on the 13th of December of the same year[2]. The Data Protection Directive was the first EU-level legal instrument, whose aim was twofold: first of all, to protect the EU citizens' data against any arbitrary and unlawful action and second to enable the safe movement of the data. The implementation of the 95/46/EC Directive across all EU member states took place three years after its effective date, a fact that is justified from the lack of harmonization among the data protection rules in EU given that the majority of the member states followed strict procedures to protect their citizens' data, while others had not shaped their own legal framework at a national level yet[3].

The Data Protection Directive, that had been implemented by the 28 EU member states, by Iceland, Liechtenstein and Norway and by Switzerland[4], was in force for 14 years when the drafting procedures for a Regulation kicked off. Although the 95/46/EC Directive promoted the main principles of the protection of the fundamental right of the EU citizens in the processing of their personal data and reached a sufficient legal uniformity level within the EU, the inconsistencies among the different national data protections rules remained an important issue that needed to be resolved.[5]

---

[1] Council Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

[2] The Privacy and Electronic Communications Directive 2002/58/EC also came into force 7 years later than the Data Protection Directive, and its main goal was to regulate more specific data-relates issues in connection with the publicly available electronic communication services such as spam, cookies etc. Natasha Lomas, *e-Privacy: An overview of Europe's other big privacy rule change* [2018], Tech Crunch, https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/ accessed on 13 December 2022

[3] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri, *Review of the European Data Protection Directive* [2009], Rand Corporation, https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dpdirective.pdf accessed on 12 December 2022 6

[4] *Overview of Privacy & Data Protection Laws: Europe*, Consumer Privacy world, https://www.consumerprivacyworld.com/privacy-europe/ accessed on 13 December 2022

[5] W. Scott Blackmer, *GDPR: Getting Ready for the New EU General Data Protection Regulation* [2016], Information Law Group, https://web.archive.org/web/20180514111300/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/ accessed on 12 December 2022 1

Rapid technological developments which created a need for an updated, strengthened legal framework for the protection of European citizens' data, as well as a fully harmonized regime for the processing and safe flow of personal data within the EU, led to the 'birth' of the 2016/679 Regulation also known as the General Data Protection Regulation[6], on the 14th of April 2016 and was enforceable to all the EU member states by the 25th of May 2018.

The new data protection legal instrument although it retained the concepts and aims of the previous Directive, introduced several new rules such as the duties and responsibilities of the data controllers and data processors, the obligation of both the data controllers and data processors to appoint a data protection officer etc. Its five most crucial goals are highlighted in the recitals 2-7 and the article 1 of the GDPR among which the protection of the data subjects' fundamental rights[7], the facilitation of the free flow of personal data within the EU, the contribution to economic progress and the legal uniformity across the EU are included.[8]

The GDPR, in contrast to its predecessor, has direct applicability and enforceability in all EU member states, obviating the necessity for additional incorporation into domestic legal frameworks. Its goal of harmonizing data protection legal regimes and eliminating differences in enforcement measures is achieved. However, member states retain the ability to introduce deviations in their national law, and not be fully compliant with GDPR. Some examples of these deviations include age limitations for minors' consent to be valid[9], the obligatoriness or not of the DPOs appointment[10], etc.

---

[6] Council Regulation (EC) 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 [2016] OJ L 119

[7] It is important to highlight that both the right to respect for private life and the right to data protection which are closely related, are dinstict and they are provided as fundamental human rights under the article 7 and article 8, respectively, of the Charter of Fundamental Rights of the European Union, EU Charter [2000] OJ C 326

[8] GDPR, recital 2-7 and article 1

[9] Ibid article 1 (b) according to which '*Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*'

[10] Ibid article 37 (4) according to which *'In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer'*

1.2. GDPR Overview

The GDPR consists of 11 chapters: The first one covers general provisions including main objectives, the scope and important definitions, the second one lays out principles for data processing and the third chapter outlines data subjects' rights. The fourth chapter deals with data controllers' and processors' obligations and the fifth one covers data transfer to third countries or international organizations. The following chapter addresses independent supervisory authorities, seventh chapter focuses on cooperation among EU member states, while the eighth one lays out remedies and penalties for non-compliance. In addition to this, the ninth chapter deals with specific processing situations, such as employment cases, while the tenth chapter covers delegated and implementing acts. The eleventh chapter, and last one, includes the final provisions of the regulation. In order to remain true and close to the dissertation's objectives, emphasis will be given to specific provisions of the GDPR and particularly to the rules that affect directly the financial institutions in order to compare the requirements provided, with the ones introduced by the AML legal instrument.

1.2.1. The Rights of the Data Subjects

As already mentioned above[11], the third chapter of the GDPR introduces the rights of the data subjects, under articles 13-22. One of the main goals of the EU data law is the privacy and autonomy of the individuals whose data are being processed within the EU. The provisions related to the specific rights of the data subjects and the circumstances under which they can be exercised could not be omitted, as they are crucial.

Pursuant to the GDPR, data subjects possess the right to be informed of the collection and use of their personal data (Article 13). Additionally, they are entitled to request access to their personal data and to obtain copies thereof (Article 15) and they have the right to have their personal data rectified if it is found to be inaccurate or incomplete (Article 16). In certain circumstances, such as when the personal data are no longer required for the purpose for which they were collected, data subjects also have the right to have their personal data erased or forgotten (Article 17). Under the GDPR article 21 data subjects possess the right to object to the processing

[11] See chapter 1.2. of the present dissertation

of their personal data (Article 21), and last but not least they are entitled to restrict the processing of their personal data (Article 18) in certain circumstances, including when they contest the accuracy of the data or when they object to its processing. An in-depth examination of the most foremost of the aforementioned rights will be discussed in the subsequent chapters with regard to financial institution clients as data subjects.

1.2.2. Legal bases for data processing under the article 6 of GDPR

The EU's data protection framework undeniably guarantees individuals a plethora of rights that offer a significant level of protection to data subjects in the digital age. However, it is worth noting that these rights can only be exercised under specific circumstances. In recognition of this, the GDPR introduced an additional mechanism to protect individuals whose data are being processed: the legal bases for lawful data processing. It is crucial for the entities to carefully consider and adhere to these legal bases in order to ensure the lawful processing of personal data. GDPR article 6 outlines six legal bases that must be considered by organizations and entities acting as data controllers or processors, one of which is *consent*.

In order to qualify as a valid form of consent, it must be specific, informed, and unambiguous.[12] This means that the individual must be fully aware of what they are agreeing to and the consequences of their consent, and must do so voluntarily without any external pressure or coercion.

Obtaining consent from an individual must be done through a clear and concise statement or request, and it must be separate from any other terms and conditions [13]. Additionally, individuals must be able to withdraw their consent at any time, and the withdrawal must be as easy as giving it. Organizations and entities must also keep a record of the consent obtained from individuals, as well as any evidence of the individual's agreement to the processing of their personal data.

---

[12] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law [2018] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition accessed on 19 December 2022, 142-143

[13] An interesting example is the consent when requested by the minors. In this case the minor's guardian is the one responsible to provide with their consent, Article 29 Data Protection Working Party, *EU General Data Protection Regulation – General Information Document* [2016], https://www.appaforum.org/wp-content accessed on 15 December 2022 3

In some cases, consent may not be the most appropriate legal basis for data processing. For example, if the processing of personal data is necessary for the performance of a contract or to comply with a legal obligation, then consent is not required.

A second legal ground for the lawful data processing is related with the performance of a contract under article 6 (1)(b) according to which the processing of personal data is permitted when it is essential for the execution of a contract to which the data subject is a party, or in order to initiate proceedings at the request of the data subject before the conclusion of a contract. This indicates that, in order to fulfill the obligations of a contract or initiate proceedings towards entering into one, it may be necessary to process the personal data of the data subject.[14]

It is crucial to emphasize that this legal basis for processing personal data is only applicable if the processing is necessary for the performance or the initial proceedings for the contract conclusion[15]. In other words, the processing must be strictly necessary for these purposes and cannot be based on the company's legitimate interests or any other legal grounds for processing.

Moreover, the compliance with a legal obligation is provided as a legal basis for the data processing under GDPR article 6(1)(c). Pursuant to the previously mentioned GDPR article the processing of personal data is permitted when it is imperative for the satisfaction of a legal obligation incumbent upon the controller. This implies that, if a company or organization is mandated by law[16] to process personal data, they may do so on the basis of this legal ground. For instance, if a company is required by tax law to maintain records of its employees' personal data, they may process this data in order to fulfill this legal obligation. Once again, the processing must be

[14] For instance, if an individual is purchasing a product online, the company may need to process their personal data (such as their name, address, and payment information) in order to fulfill the purchase and deliver the product.

[15] European Data Protection Board, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [2019], https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed on 21 December 2022 8.

[16] With the term *law,* primary legislation, secondary legislation and common law are covered. Data Protection Commission, *Guidance note: Legal Bases for Processing Personal Data* [2019], https://www.dataprotection.ie/sites/default/files/ accessed on 21 December 2022 14

essential for achieving the stated purposes, and cannot be justified by the controller's self-serving interests or any other legal justifications for processing.

Another legal basis according to the GDPR is the protection of the vital interests of the data subject or other natural person, under article 6(1)(d). If the processing of personal data is necessary to safeguard the life, health, or well-being of an individual, it may be permitted on this legal ground. Undoubtedly, the specific legal justification covers necessity and emergency situations which a proportionate examination test must take place at, in order to protect the interests that are essential for life, but with a less intrusive way possible.[17]

Data processing may be imperative for the execution of a task undertaken in the public interest or as a result of official authority vested in the controller, under GDPR article 6(1)(e). This legal justification is based on the notion that certain activities, such as those related to public health, criminal justice, or education, are essential to the functioning of society and therefore require the use of data processing to be carried out effectively. It refers specifically to public authorities or legal or natural persons governed by the public law when they act as data controllers.[18]

Last but not least, in accordance with article 6(1)(f) the processing of personal data is permissible on the basis of legitimate interests pursued by the controller or by a third party. This means that the processing is justifiable if it is necessary for the legitimate interests of the controller or third party, provided that the rights and freedoms of the data subject are not disproportionately compromised by such processing.[19] Legitimate interests may encompass the interests of the controller or third party in conducting their affairs, enhancing their products or services, or safeguarding their own interests. Nevertheless, the controller or third party must weigh and balance the potential impact on the data subject's privacy rights prior to relying on this legal ground.

In conclusion, it is evident that the legal grounds for data processing under GDPR article 6 are multifaceted. The regulation places a significant emphasis on ensuring that personal data are processed in a manner that is both lawful and transparent, and it provides a number of specific legal grounds that can be relied upon to

[17] Ibid 17

[18] Data Protection Commission 20

[19] Ibid 21

legitimize such processing. The grounds, as already mentioned, include consent, contract, legal obligation, vital interests, public task, and legitimate interests, and each of the bases has its own specific requirements and limitations. Overall, it is crucial for organizations to carefully consider the legal grounds that apply to their data processing activities in order to ensure compliance with the data protection regime.

1.3. GDPR application in the Financial Sector

The financial sector is one of the many industries that is heavily impacted by the GDPR. Financial institutions, such as banks and insurance companies, handle a large amount of personal data on a daily basis making them prime targets for data breaches and cyber-attacks. Therefore, they are subject to the GDPR's strict requirements not only for their customers' personal data, but for their employees, as well.

Regarding the financial data that are requested and processed by financial institutions, they refer to information that relates to an individual's financial affairs, such as bank account details, credit card information, salary or income information, and other financial transactions. It is worth emphasizing that this category of data is deemed to be categorized as sensitive data, and may necessitate supplementary safeguards due to the possibility of harm or prejudice if handled or exploited improperly, although it is not explicitly included among the special data categories under GDPR article 9. However, in the author's opinion, the definition of sensitive data under the GDPR according to which they are personal data *that reveal 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*[20] may not refer directly to financial data, but it could be argued that it covers them as well, since the latter reveal political opinions, religious or philosophical beliefs, or trade union membership and therefore could potentially reveal sensitive information about an individual.

[20] GDPR article 9

It is of importance to note that, there are specific data protection rules that have been adopted at an EU level which cover the special case of financial data[21] and specifically those are the Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments[22], the Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories[23], the Regulation (EC) No 1060/2009 of the European Parliament and of the Council on credit rating agencies[24], and last but not least the Directive 2007/64/EC of the European Parliament and of the Council on payment services in the internal market[25].

Last but not least, regarding the scope of application, the GDPR applies to all organizations including those based outside the EU, that process the personal data of EU citizens, and it imposes strict requirements on these organizations with regard to the collection, use, storage, and protection of personal data. Therefore, it is important to note that the GDPR applies regardless of the physical location of the organization, in accordance with the territorial scope of the regulation.[26]

1.3.1. The Role of Financial Institutions as Data Controllers: Duties and Responsibilities

The safeguarding of personal data has become a critical concern for both individuals and organizations in the digital age, as an increasing amount of data is being shared

---

[21] European Union Agency for Fundamental Rights and Council of Europe 326

[22] European Parliament and Council, *Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU* [2014], OJ L 173/349, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML accessed on 22 December 2022

[23] European Parliament and Council, *Regulation (EU) No 648/2012 of 4 July 2012 on OTC derivatives, central counterparties and trade repositories* [2012], OJ L 201 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0648 accessed on 22 December 2022

[24] European Parliament and Council, *Regulation (EC) No 1060/2009 of 16 September 2009 on credit rating agencies* [2009], OJ L 302 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R1060 accessed on 22 December 2022

[25] European Parliament and Council, *Directive 2007/64/EC of 13 November 2007 on payment services in the internal market* [2007], OJ L 319 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0064 accessed on 22 December 2022

[26] Under GDPR article 3(1). This means that even if an organization acting as a data controller or processor is based outside of the EU, it must still comply with the GDPR rules if it processes personal data of individuals within the EU, European Data Protection Board, *Guidelines 3/2018 on territorial scope of the GDPR (Article 3)* [2020], https://edpb.europa.eu/sites/default/files accessed on 10 January 2023 4

and stored online. To ensure the security and confidentiality of this information, effective measures must be implemented. Therefore, among other organizations and entities, financial institutions have the legal obligation, when acting as data controllers, to properly handle and protect the data they collect and process. This includes implementing security measures to prevent unauthorized access or misuse of the data and adhering to relevant laws, particularly the GDPR. In this chapter, we will delve into the role of financial institutions as data controllers and explore the various responsibilities that come with this role. Taking into account that there is a wide range of duties that financial institutions may be required to fulfill under the GDPR provisions, depending on the specific circumstances of their operations and the type of personal data they collect and process, we will focus on the most significant ones:

A. Compliance with the Data Minimization principle

It is important to note that the data minimization principle[27] is a key consideration at the outset. This necessitates the strict necessity for the collection, processing, and retention of personal data solely for the purpose of the specific financial services being provided. For instance, a bank may be required to gather personal data such as an individual's name, address, and financial information in order to open a new account. However, the bank would not be permitted to collect or retain additional personal data not necessary for this purpose unless explicit consent has been obtained from the individual in question.

The GDPR's principle of data minimization stipulates that personal data must be *adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed*. This principle is further expounded upon in Article 25, which dictates the implementation of measures to ensure the minimal intrusiveness of personal data collection and processing, as well as the retention of said data solely for the duration required to fulfill the specific purpose for which it was originally collected.[28] Consequently, financial institutions serving as data controllers must carefully evaluate the personal data requested from their clients in order to determine the purpose for which they are being collected, identify any alternative

[27] Article 5 sets out the principles of data protection, one of which is data minimization, GDPR article 5

[28] European Union Agency for Fundamental Rights and Council of Europe 126

means for achieving that purpose, and establish a time frame for retaining the data within their systems.[29] This necessitates their responsibility to implement suitable technical and organizational measures in order to secure and preserve the confidentiality of personal data and be open and transparent[30] about their data collection and processing practices. It is of the utmost importance that they take their obligations under the GDPR seriously and strive to adhere to the principle of data minimization in order to avoid significant fines and reputational damage.

B. Adoption of data protection technical and organizational measures

Since we referred to technical measures in relation with the data minimization, it is important to focus further on them with the relevant references in the articles of the regulation. GDPR article 32 sets out the requirements for the security of personal data processing. It states that data controllers and processors in general, and therefore the financial institutions, must implement appropriate technical and organizational measures that will depend on the nature of the personal data being processed, the risks posed by the processing, and the costs of implementing different security measures. Some examples of technical and organizational measures that may be appropriate and are explicitly provided in article 36, are the encryption[31] of personal data to protect them from unauthorized access or disclosure, the implementation of secure access controls to prevent unauthorized access to personal data[32], regular updating of security protocols and software to protect against emerging threats, adoption of measures to ensure the availability and resilience of systems and services used to process personal data and last but not least implementation of measures to restore the availability and access to personal

[29] All the steps in a detailed way given in Protecto, *Data Minimization: Checklist, strategies and steps*, https://www.protecto.ai/wp-content/uploads/2022/01/Data-Minimization-Strategies-and-Steps-Protecto.pdf accessed on 22 December 2022

[30] In recital 39 of the GDPR the importance of data minimization is also underlined, GDPR recital 39

[31] Data encryption is a process that involves converting plain, unencrypted data into a secure, encrypted form using a mathematical algorithm and a secret key. The encrypted data, also known as ciphertext, is difficult or impossible to interpret without the key. Data encryption is an effective and the most famous way to secure data and can be used in a variety of contexts, including for data storage, data transmission, and data backup, Juliana De Groot, *What Is Data Encryption? Definition, Best Practices & More* [2015] https://digitalguardian.com/blog/what-data-encryption accessed on 22 December 2022

[32] This measure may include the use of passwords, security tokens, or other authentication methods which is very common

data in a timely manner in the event of a physical or technical incident.[33] Every financial institution must examine all the circumstances and shape its own data privacy risk framework in order to take all the appropriate measures according to its needs, balancing the implementation costs, the data subjects' rights and the state of the art. GDPR specifically refers to conducting a privacy risk assessment, also known as a risk-based approach, when implementing measures to protect personal data in accordance with Article 32.[34]

C. Respect of data subjects' rights

In subchapter 1.2.1. a brief analysis of the data subjects' rights took place. Among the financial institutions' obligations under the GDPR, the respect and safeguard of their clients' rights as data subjects, including the right to erase, access, modify and restrict the processing of personal data, is of utmost importance. As such, it is incumbent upon financial institutions to furnish individuals with suitable information and assistance to enable the exercise of these rights. To this end, it is the financial organizations' duty to establish protocols for addressing requests related to data subject rights and for addressing the respective requests expediently and appropriately. The failure to respect data subject rights can result in regulatory penalties being imposed by data protection authorities. A short list of these rights is set out in the 1.2.1. section above however it is essential to focus on a few of them, mainly due to the fact that when they are exercised by data subjects - customers they may cause difficulties for financial institutions to remain compliant with both the GDPR and AML frameworks, as we will examine in the third chapter. First of all, according to GDPR article 17, every individual has the right to request from the respective data controller to erase any kind of data or information collected and stored related to themselves[35] if there is no compelling reason for the data to be retained[36]. The *right to erasure*, or the *right to be forgotten*[37], is not absolute, and it

[33] GDPR article 32

[34] Annika Selzer, Daniel Woods and Rainer Böhme, *Practitioners' Corner - An Economic Analysis of Appropriateness under Article 32 GDPR* [2021], European Data Protection Law Review, Volume 7, Issue 3, https://edpl.lexxion.eu/data/article/17705/pdf/edpl_2021_03-016.pdf accessed on 22 December 2022 456

[35] Including any copies or duplicates of the data that may exist.

[36] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies* [2017],

may be limited in certain circumstances, for instance it is not applicable if the processing of the personal data is necessary for the exercise of the right of freedom of expression and information, for the performance of a task carried out in the public interest, or for the establishment, exercise, or defense of legal claims. It definitely gives the data subjects the chance to obtain the control of their rights and demand their erasure from the data controllers' records *without undue delay.*

The right to *data portability*, recognized under GDPR article 20, affords individuals the ability to obtain their personal data in a *structured, commonly used, and machine-readable format*, as well as transmit said data to another controller without impediment. It is applicable when the processing of personal data is based on consent or a contract, and is carried out through automated means. The principal objective of the right to data portability is to empower individuals and enable them to assert control over their personal data[38]. It enables them to easily migrate, duplicate, or transfer their data from one service provider to another, without being bound to a specific service. Financial institutions' obligation is to provide their clients with information on how to exercise their right to data portability, and must respond to requests within one month, unless the request is particularly complex or the controller has received a high number of requests.

According to article 21 data subjects have *the right to object* to the processing of their personal data at any time, for reasons related to their particular situation. This right applies to any type of processing, including processing for direct marketing purposes, and if it is exercised by their clients, the financial institutions must no longer process their personal data, unless they demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the

---

Computer Law & Security Review: The International Journal of Technology Law and Practice, doi: 10.1016/j.clsr.2017.05.015

[37] The right to erasure was one of the innovations introduced for the first time with the Regulation while not falling under the Data Protection Directive. It was first discussed in 2014, before the adoption of the GDPR, on the Court of Justice of the European Union in the case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González according to which Gonzales, a Spanish citizen asked the deletion of his name and any kind of information of him related to the sale of his property due to social security debts, since all those information were outdated and no longer relevant to him, Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] OJ C212/4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CA0131

[38] European Union Agency for Fundamental Rights and Council of Europe 229

individual, or for the establishment, exercise, or defense of legal claims. It worth to be noted that financial organizations must provide concise information about the right to object in their privacy notices ensuring that their clients are able to easily exercise it.[39]

Another significant right granted to data subjects which financial institutions must respect is the *right to access*. The right to access, provided under GDPR article 15 grants individuals the authority to request and obtain confirmation as to whether or not personal data concerning them are being processed, as well as access to said data and information regarding the processing thereof. Thus, financial institutions are obligated to provide a copy of the personal data undergoing processing, free of charge, in an electronic format that is commonly used.[40] They are also required to provide individuals with information on the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, and the envisaged period for which the personal data will be stored.

In conclusion, the data subject rights recognized under the EU data protection framework are of paramount importance and any failure to adhere to the respective GDPR's provisions can result in significant penalties. Consequently, it is imperative that financial institutions prioritize the protection of personal data and the fulfillment of data subject rights, investing in systems to effectively respond to requests, in order to maintain their customers' trust.

D. Legal Bases for Data Processing

It is important to note that financial institutions must be able to demonstrate that they have a valid reason for collecting, using, storing and generally processing of their clients' personal data, and provide evidence of this legal basis upon request. Financial institutions should carefully consider which legal basis is most appropriate for their processing activities. All the six legal grounds provided by the GDPR in article 6(1) have been analyzed in detail in the preceding sub-chapter 1.2.2.

[39] Ibid 230

[40] The right to access is subject to certain exemptions, such as when the disclosure of the requested information would adversely affect the rights and freedoms of others, ibid 217

E. Data protection by design and by default

The GDPR introduces among others the concepts of data protection *by design* and data protection *by default*. In order to be compliant with the first one under article 25[41] financial institutions must adopt a data protection-by-design approach, meaning that they must incorporate data protection considerations into the design of their products and services.[42] This includes designing systems, processes, and products that minimize the collection and processing of personal data, and that ensure the confidentiality, integrity, and availability of personal data.

In addition, and regarding the second concept, financial institutions must ensure that data protection is the default setting, as stipulated under GDPR article 25(2). This means that individuals must take affirmative action to allow their data to be processed, rather than having to opt out of data processing.[43] For instance, if a financial institution wants to use personal data for marketing purposes, it must obtain the explicit consent of the individual before doing so. This helps to ensure that individuals have control over their personal data and that it is not processed without their knowledge or consent.

The data protection-by-design and by-default approaches impose the aforementioned obligation to financial institutions, ensuring that the latter are proactive in protecting the personal data of their customers and clients, and mainly transparent about how they use personal data, preventing data breaches and other security incidents, as they require financial institutions to design their systems and processes with data protection in mind.

F. Data Protection Impact Assessments (DPIAs)

Data protection impact assessments (DPIAs) are a key aspect of the GDPR and designed to help financial institutions, when acting as data controllers, to identify and address potential data protection risks before they occur. Under Article 35, financial institutions are required to conduct DPIAs in certain circumstances, such as

[41] GDPR article 25

[42] European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* [2020], https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904.pdf accessed on 23 December of 2022 6

[43] Ibid 11

when introducing new processing activities that are likely to result in a high risk to the rights and freedoms of their clients.

More specifically DPIAs involve a systematic and structured process that includes identifying the personal data that will be processed, evaluating the potential risks to the subjects' rights, and determining the measures that can be taken to address them. It is important for financial institutions to be aware of the requirements for conducting DPIAs and to have systems in place to effectively conduct and document them.[44]

G. Data Protection Officer Appointment

As underlined under article 35(2) about the DPIA: *the controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*[45]Even from this section the importance of a Data Protection Officer (DPO) appointment is highlighted. A DPO serves to guarantee that financial institutions fulfill their obligations under GDPR and implement measures to safeguard of their clients' personal data.[46] By serving as a resource on matters related to data protection, a DPO can furnish professional counsel on such issues and assist financial institutions in identifying and addressing any potential vulnerabilities to the confidentiality and personal data of their clientele. Appointing a DPO is not obligatory in every case. According to article 37[47] there are certain circumstances in which a controller or processor must appoint a DPO. These include: the processing of personal data when carried out by a public authority or body (excluding courts acting in their judicial capacity); If the controller or processor's core activities involve regular and systematic monitoring of data subjects on a large scale due to the nature, scope, and/or purposes of the processing operations; if the controller or

[44] According to article 35(7) the DPIAs must have specific contents which at least include: *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned,* GDPR article 35(7).

[45] GDPR article 35(2)

[46] Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula 11

[47] GDPR 37(1)

processor's core activities involve processing on a large scale of special categories of data or personal data related to criminal convictions and offenses. Consequently, it is up to data controllers and processors to assess the necessity for appointing a DPO based on the unique characteristics of their data processing operations.[48] Nevertheless, due to the inherent nature of their operations and mainly the processing of sensitive data, such as financial and banking records, financial institutions are in many instances obligated to appoint a DPO in compliance with the GDPR.

The previously enumerated list constitutes but a sample of the extensive obligations that financial sector organizations must comply with under the GDPR. The role of financial institutions as data controllers is of paramount importance, entailing a substantial degree of accountability. Being required to handle large amounts of personal data, including sensitive information, they may often need to transfer such data across national borders for various reasons, including processing by third-party service providers. The GDPR regulates these cross-border data transfer activities, aimed at preserving individuals' rights and freedoms, by ensuring an equivalent level of data protection within the EU. By instituting a framework for cross-border data transfers, it establishes a standard of data protection that applies to all organizations operating within the EU, regardless of their physical location[49].

2. EU ANTI-MONEY LAUNDERING DIRECTIVE

Having conducted an examination of the main provisions of the GDPR in chapter 1, the following one will undertake an analysis of the most significant provisions of the Anti-Money Laundering Directives and the EU regulatory framework. A brief historical overview, a reference to the rules provided and a review of the requirements that must be fulfilled by the financial institutions will follow. Subsequent to this, we will have the opportunity to compare the two frameworks

[48] A controller or processor may also choose to appoint a DPO on a voluntary basis even if they are not obliged to do so, European Union Agency for Fundamental Rights and Council of Europe 176

[49] As highlighted above regarding the territorial scope of application of the GDPR, see chapter 1.3. of the present dissertation

and evaluate whether the provisions of the two pieces of legislation are conflicting and to what extent there is an impact on the financial organizations.

2.1. Historical Background

The EU has had a longstanding commitment to combating money laundering and terrorist financing. This commitment is reflected in the Anti-Money Laundering (AML) regulatory framework, which has evolved over time to meet the changing needs and challenges of the financial sector[50]. The first EU AML Directive[51] was adopted in 1991[52], following the recommendations of the Financial Action Task Force (FATF), an intergovernmental organization that develops and promotes policies to combat money laundering and terrorist financing. The Directive established minimum standards for AML measures, including customer due diligence and record-keeping requirements, and established a system for the exchange of information between EU member states. Since its inception, the EU AML regulatory framework has undergone several updates and amendments. The Second AML Directive, also known as the AMLD2[53] was adopted in 2001 in response to the September 11th terrorist attacks and the increased risk of terrorist financing, with the aim to fill the gaps of the first one. It expanded the scope of the First AML Directive to cover a wider range of financial institutions and designated businesses and professions, introducing new measures to prevent the misuse of new payment methods, such as prepaid cards and electronic money. Following the 2nd, the Third AML Directive

---

[50] European Court of Auditors, *The EU's anti-money laundering policy in the banking sector* [2020], https://www.eca.europa.eu/lists/ecadocuments.pdf accessed on 24 December 2022

[51] The AML scheme throughout the EU is primarily stem from the AML Directives which establish specific goals that member states must meet, but allow them to choose how they will achieve them with the Directives implementation into their national legislation, Council of Bars and Law Societies of Europe, *Efficiency in anti-money laundering regulation - The path to combating the laundering of proceeds of crime effectively* [2020], The voice of European Lawyers, https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/ANTI_MONEY_LAUNDERING/AML_Position_papers/EN_AML_20200626_Efficiency-in-anti-money-laundering-regulation-The-path-to-combatting-the-laundering-of-proceeds-of-crime-effectively.pdf accessed on 24 December 2022 3

[52] European Council *Directive (EC) 91/308 on prevention of the use of the financial system for the purpose of money laundering* [1991] OJ L166/77 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31991L0308 accessed on 24 December 2022

[53] European Council *Directive (EC) 01/97 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering* [2001] OJ L344/76 https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF accessed on 24 December 2022

(AMLD3)[54], was adopted in 2005 replacing the former one four years later, in response to the growing risks posed by money laundering and terrorist financing, therefore it introduced new requirements for customer due diligence and the identification and verification of the customers' identity. The Fourth Anti-Money Laundering Directive (AMLD4)[55], which was adopted in 2015 and entered into force in June 2017 was the one that introduced a number of significant changes to the EU AML regulatory scheme, including the expansion of Directive's scope to cover new types of financial institutions, such as virtual currency exchanges and custodian wallet providers. AMLD4 paved the way for the adoption of AMLD5. The AMLD5[56] which was adopted in 2018 and came into force in 2020[57], strengthens and updates the measures established by the AMLD4 in order to better address the evolving risks of money laundering and terrorist financing. Particularly, AMLD5 builds upon its predecessor[58], rather than replacing it entirely, since the former supplements, updates and adds new provisions and requirements to the latter.[59] Both the Directives operate in close collaboration, with the latter updating and adding to certain provisions of the former and revising the overall legal framework. The AMLD5

---

[54] European Council *Directive (EC) 2005/60 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* [2005] OJ L309/15 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060 accessed on 24 December 2022

[55] European Council *Directive (EC) 2015/849 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 L141/73 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849 accessed on 24 December 2022

[56] European Council *Directive (EC) 2018/843 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 L156/43 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843 accessed on 24 December 2022

[57] EU member states were required to implement the AMLD5 into their national laws by December 10, 2020.

[58] It should be noted that there is also the Council Directive (EC) 2018/1673 on combating money laundering by criminal law which establishes common minimum rules concerning the definition of criminal offenses and sanctions in the area of money laundering. It was adopted in 2018 and came into force in 2019. It is considered to be the 6th AMLD, e.g. Comply Advantage *6AMLD: 6th Money Laundering Directive,* https://complyadvantage.com/insights/6th-money-laundering-directive-6amld/ accessed on 24 December 2022

[59] Marek Kot, *Impact of the 5th Anti-Money Laundering Directive on EU's financial market,* Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges, 11641

specifically recognizes the importance of the Fourth in its recitals[60], stating that it serves as the primary means of preventing financial crimes. Henceforth, this dissertation will focus on the provisions of both the AMLD4 and AMLD5 as the latter's provisions are constructed upon the rules of the former and it is essential in order to provide a complete and accurate picture of the whole regulatory framework governing the obligations of the financial institutions with respect to money laundering.

2.2. AMLD4/AMLD5 Overview

AMLD4 and AMLD5 aim to ensure that the EU's financial system is not exploited for illicit purposes and to protect against the risks of money laundering and terrorist financing. The AMLD4 established a series of measures among which the most significant include the requirement for financial institutions and other designated businesses and professions (such as lawyers, accountants, and real estate agents) to perform customer due diligence, including identifying and verifying the identity of their customers and assessing their money laundering and terrorist financing risks[61]; the requirement for financial institutions and other designated businesses and professions to report suspicious activities to national financial intelligence units (FIUs) in the member states where they operate[62]; the empowerment of the EU institutions, among others the EU Commission, to adopt delegated acts to identify high-risk third countries, - which are jurisdictions that pose significant threats to the financial system of the EU taking into account various factors, including the legal and institutional AML framework, the powers and procedures of the country's competent authorities, and the effectiveness of the country's AML system[63]-; the requirement for member states to establish central registers or other systems for the identification of the beneficial ownership of companies and trusts[64].

[60] European Council Directive (EC) 2018/843 recital (1)

[61] AMLD4 article 3

[62] AMLD4 article 4

[63] AMLD4 article 9

[64] AMLD4 article 30

As already highlighted above, the provisions of the AMLD5 were based and built on the AMLD4 ones. Among the amendments that the AMLD5 introduced to the protection against money laundering scheme, the following are included[65]:

The scope expansion of the Directive to cover virtual currency exchange platforms and custodian wallet providers, as well as tax advisors, art dealers, and other professionals who engage in transactions involving high sums of cash[66] is one of the main additions.[67] This expansion of the scope of AMLD5 aims to ensure that these new types of businesses and professions are subject to the same anti-money laundering and terrorist financing requirements as other financial institutions and designated businesses and professions[68]. By requiring these businesses and professions to comply with AMLD5's provisions, authorities can better monitor and prevent the use of these sectors for illicit purposes.

Moreover, AMLD5 introduced provisions for the assessment of risks posed by higher-risk third countries and politically exposed persons (PEPs).[69] As part of these rules, AMLD5 requires Member States to issue a list of specific functions that qualify as *prominent public functions* to identify PEPs for monitoring. The EU will then consolidate the lists from the member states and publish the results anonymously. Additionally, AMLD5 requires enhanced due diligence measures for high-risk third countries, including obtaining information on the source of funds, background checks, and beneficial ownership. Last but not least, member states may proscribe firms from opening branches or subsidiaries in high-risk third countries and may impede the opening of a branch or subsidiary of a firm that is headquartered in a high-risk third country. The ultimate objective of these measures is to harmonize the regulations concerning high-risk jurisdictions across EU and to encourage firms to limit their relationships with these countries.

---

[65] An indicative list of the most significant ones is set out.

[66] AMLD5 article 2

[67] It is worth noting that before the amendment of AMLD5, AMLD4 mainly focused on the traditional financial institutions, such as banks, credit institutions and financial companies, and also included other designated businesses and professions, like casinos, but did not cover virtual currency and other non-financial businesses and professions.

[68] Dr. István László Gál, *The 2018/843 EU Directive on the prevention of money laundering and terrorist financing and its correlation to the criminal law prevention of the stock markets* [2019] available at http://real.mtak.hu/ accessed on 23 December 2022 116

[69] AMLD5 article 4

Another addition to the AML regulatory scheme that the AMLD5 introduced are the provisions with the aim to enhance the powers of national financial intelligence units (FIUs) and the cooperation between them[70] in order to improve the ability of authorities to detect and investigate suspicious activities and to take appropriate action to prevent money laundering actions.

Undoubtedly the above constitute only a small list of the new provisions introduced by the AMLD5, which for reasons of briefness will not be analyzed further. Namely some additional amendments are related to the requirement of member states to establish rules on the freezing and confiscation of proceeds of crime and to ensure that they have the necessary powers and means to identify, trace, and freeze or seize proceeds of crime and instrumentalities[71]; the requirements of the member states to ensure that their national laws provide for sanctions for natural and legal persons, including criminal and non-criminal sanctions, for breaches of the provisions of AMLD5[72]; new requirements for the supervision and enforcement of the Directive, including the establishment of independent and effective supervision authorities, the powers of these authorities, and the procedures for cooperation between them[73] etc.

2.3. Know Your Customer Requirements – Financial Institutions Obligations

In the modern financial landscape, the prevention of money laundering and terrorist financing is of paramount importance, as already pointed out. To this end, financial institutions are required to implement Know Your Customer (KYC) requirements, which are designed to enable them to identify and verify the identity of their customers, as well as to assess the risks associated with doing business with them and ensure that a business is not engaging with individuals connected to illegal activities such as terrorism, corruption, or money laundering. These requirements are outlined in various laws, regulations, and industry standards and are intended to help financial institutions detect and prevent illicit financial activity. The dichotomy between AMLD and the KYC lies in the fact that the former represents the broad concept of combating illicit financial activities in EU, whereas KYC constitutes the

[70] AMLD5 article 7

[71] AMLD5 article 16

[72] AMLD5 article 18

[73] AMLD5 20-24

means to attain that objective. It is worth noting that the KYC obligations of financial institutions are not static, but rather are subject to ongoing evolution in response to changes in the financial landscape and the increasing sophistication of money launderers and other financial criminals. Ultimately, the goal of this subchapter is to provide a comprehensive overview of the KYC requirements that financial institutions must follow in order to ensure compliance with AMLD, and afterwards to examine those obligations in relation with the EU data protection framework.

A. Customer Identification Program

Pursuant to the AMLD4 provisions, financial institutions and other regulated entities are mandated to establish and implement a Customer Identification Program (CIP) as an integral component of their Customer Due Diligence (CDD) procedures. The CIP is a series of protocols designed to verify the identity of customers and any relevant beneficial owners when they enter into a business relationship or carry out a single transaction exceeding certain thresholds. The stipulations of the CIP are outlined in AMLD4 Article 8, which obliges financial institutions to structure a specific policy in order to collect and process certain identifying data from customers, including name, date of birth, place of birth, nationality, and address. Financial institutions may also be required to verify evidence of customer identity, such as a passport or national identification card. In addition, financial institutions must have systems in place to confirm the accuracy of collected information and detect any discrepancies or inconsistencies, or establish specific procedures to handle situations where they are unable to verify the identity of a customer, such as when the customer is unable to provide sufficient identification documents. These measures are without doubt designed to help prevent financial crimes and consitute an important part of the overall efforts to maintain the integrity and stability of the financial system.

B. Customer Due Diligence

Once the financial institution has identified and verified the identity of its customers, it is required to conduct Customer Due Diligence (CDD)[74] to assess the money laundering and terrorist financing risks associated with the customer and the business relationship. CDD includes ongoing monitoring of the business relationship to ensure that it is consistent with the information obtained during the CIP. AMLD4

[74] Customer Due Diligence rules are provided under the Chapter II, Section one of the AMLD4, and particularly under articles 10-14

Article 13 sets out the CDD requirements for financial institutions, which include obtaining and verifying the customer's identity, identifying and verifying the beneficial owner, assessing the purpose and nature of the business relationship, and conducting ongoing monitoring of the business relationship to ensure transactions are consistent with the customer's known profile and risk profile.[75] This may include scrutiny of transactions and updating customer information as necessary. In conclusion, the CDD requirements outlined in AMLD4 serve to assist financial institutions and other regulated entities in identifying and evaluating the hazards linked to their customers.

C. Enhanced Due Diligence

In some cases, financial institutions may be required to conduct Enhanced Due Diligence (EDD) to mitigate the risks of money laundering and terrorist financing. EDD involves additional measures beyond CDD, such as enhanced monitoring and record-keeping, to ensure that the financial institution has a higher level of understanding of the customer and the business relationship.

AMLD4 Articles 18-24[76] set out the circumstances in which financial institutions are required to conduct EDD, which include situations where the customer is located in a high-risk third country, the customer is a politically exposed person (PEP), or the business relationship or transaction involves a higher level of risk. Financial institutions are also required to report any suspicious activity to the relevant national financial intelligence unit in these cases. Through EDD, the obliged entities can take appropriate measures to manage and mitigate any identified risks with a deeper understanding of their customers and business relationships.

Overall, KYC requirements, as underlined above, play a critical role for the EU AML framework as they prevent the use of the financial system for illicit purposes and they help to maintain the trust and confidence of the general public in the financial system, which is essential for the proper functioning of the economy.

[75] Under AMLD4 article 13(1)

[76] Enhanced Due Diligence rules are provided under the Chapter II, Section three of the AMLD4 and particularly under articles 18-24

3. DATA PROCESSING BY THE FINANCIAL INSTITUTIONS IN THE LIGHT OF GDPR AND AMLD

In the previous chapters the main provisions of the Data Protection and the Anti-Money Laundering framework in the EU were analyzed and the principal procedures explained. The processing of personal data has become an increasingly fraught topic, with the GDPR and AMLDs both seeking to regulate and protect the interests of both the data subjects and the financial institutions acting as data controllers, that are obliged to remain compliant. However, these two pieces of legislation are not always in alignment, leading to potential conflicts in their implementation. The following chapter will delve into the specific areas where such conflicts may arise, examining the ways in which the GDPR and AMLD intersect and potentially collide in their attempts to safeguard personal data[77].

3.1. Scenarios of potential conflicts between the GDPR and the AMLDs with respect to personal data

In subchapter 1.2.2. an analysis on the legal grounds, which any financial institution, when acting as a data controller, must invoke in order for the data processing to be lawful, takes place. Therefore, the GDPR imposes strict limitations on the collection and processing of personal data, and requires that it must be done in a fair and lawful manner. On the other hand, the AMLDs require from the financial institutions to gather all the data and information needed for the identification and verification of their clients for the purposes of combating money laundering and terrorist financing. To summarize, one of the key differences between the GDPR and the KYC requirements under the AMLDs is the *purpose* for which personal data is collected and processed. Under the GDPR, personal data can only be collected and processed for specific, legitimate purposes, such as the consent from their client or the performance of a contract or the protection of the legitimate interests of the data controller[78]. The biggest challenge is the client consent. This effectively means that the financial institution as a data controller or processor must possess and demonstrate evidence of freely-given, valid, informed, and explicit, unambiguous

[77] It is worth noting that the list is indicative and it covers the most significant conflicts between the two legal instruments

[78] See sub-chapter 1.2.2. and 1.3.1.D. of the present dissertation

consent from the data subject in order to process the personal data of a data subject. In the realm of institutional banking, this will involve shareholder and beneficial owner data, among others. Obtaining explicit consent is a significant requirement, among the other legal grounds, forcing banks to fundamentally reconsider the way in which they collect and manage customer data.[79] In contrast, the KYC requirements under the AMLD4 require financial institutions to collect and process personal data in order to comply with their AML obligations, regardless of the specific purposes for which the data is collected. Undoubtedly, this can create a conflict with the AMLDs' requirements to collect and process personal data for the purposes of combating illegal financial actions, which may not always align with the legal bases for processing set out in the GDPR[80]. A counterpoint that can be proffered to this is that the *legal obligation* constitutes a valid legal basis under GDPR that can be used by financial institutions to collect and process personal data for the purposes of complying with their AML obligations without the need to obtain explicit consent from data subjects. This is accurate as long as they can establish that the collection and processing of personal data is imperative to comply with the legal obligation and that they take into account the principles of data minimization and proportionality. Undeniably, the legal obligation ground must be employed in accordance with the GDPR principles, and a test of proportionality must be conducted to ascertain that it is the most suitable in specific situations.

A second potential conflict between the AML scheme and the GDPR rules relates to the right to be forgotten also known as the right to erasure[81]. Under the GDPR, individuals have the right to request the erasure of their personal data in certain situations, such as when the data is no longer necessary for the purposes for which it was collected or when the individual revokes their consent for the processing of their data. Financial institutions must comply with these requests and erase the relevant personal data, unless there are valid legal grounds for retaining it. However, the AMLD requires financial institutions to retain customer due diligence records for at

---

[79] Laura Glynn, *KYC vs Data Protection – The next compliance hurdle* [2016] Fenergo 11

[80] Bernadine Reese, *GDPR and EU AML Directives – A Regulatory Tug-of-War?* [2018], Protiviti Global Business Consulting https://blog.protiviti.com/2018/05/24/gdpr-eu-aml-directives-regulatory-tug-war/ accessed on 30 December 2022

[81] See sub-chapter 1.2.1. of the present dissertation

least five years after the end of the business relationship.[82] This may create a conflict with the GDPR's right to erasure, as financial institutions may be required to retain personal data for a longer period than what the GDPR permits[83]. A key issue that needs to be taken into account is whether the data retention requirement outlined in the AMLD can be deemed appropriate in relation to the objectives it seeks to accomplish. The proportionality principle requires that the actions taken be both effective and necessary, meaning that the goal could not be achieved through less invasive means. While the fight against financial crime is certainly vital, it must be balanced against the significant invasion of privacy for every individual who is a bank's customer. The Directive's provisions result in the accumulation and preservation of data that may be interesting but not necessarily essential for extended periods of time.[84]

Another area where this tension between the two legal texts arises is with regards to the sharing of client data with third countries. Particularly, AMLD4 includes several provisions that require firms to share data with foreign regulators in order to comply with the Directive's newly extended reporting obligations. These provisions, specifically articles 39, 42, and 45, also require firms to establish policies for sharing data across group companies located in third countries for AML and counter-terrorist financing (CFT) purposes. Moreover, article 39(3) and 39(5) outline the circumstances under which obliged entities, such as financial institutions, may share certain types of information, such as Suspicious Activity Reports (SARs), with other obliged entities in a third country.[85] These circumstances include the requirement that the other entity is located in a third country with equivalent AML laws, that the entities are in the same professional category, and that they are subject to data protection obligations in their jurisdiction. The aforementioned provisions are intended to ensure that financial institutions, among other obliged entities, can

---

[82] AMLD4 article 40(1)(a) according to which *in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction.*

[83] Ibid Bernadine Reese

[84] Jonida Milaj - Carolin Kaiser, *Retention of data in the new Anti-money Laundering Directive — 'need to know' versus 'nice to know*' [2017] 7(2) International Data Privacy Law https://doiorg.db.ub.oru.se/10.1093/idpl/ipx002 accessed on 3 January 2023 124

[85] Cooley - Legal insight for market innovators, *GDPR and AML – a perfect pair?* [2018] https://cdp.cooley.com/gdpr-and-aml-a-perfect-pair/ accessed on 3 January 2023

effectively cooperate with each other. On the other hand, the GDPR aims to limit personal data sharing with third countries in order to protect the privacy rights of individuals.[86] Particularly it establishes strict requirements for data transfers to third countries, and it allows such transfers only in certain specific circumstances[87]. In conclusion financial institutions are required to share their clients' data with third countries under the AML scheme and on the other hand they must respect their clients' privacy rights and comply with the GDPR's restrictions on data transfers to third countries. Balancing these competing obligations can be difficult, and it is important for financial institutions to adopt appropriate measures to ensure compliance with both regulations.

The processing and the requirements under which the former must take place by the financial institutions constitute another conflicting area between the two legal instruments. The provisions outlined in GDPR articles 13(1) and 14(1) mandate that individuals must be apprised of particular aspects regarding the processing of their personal data, including the purposes for which it will be utilized and the legal justification for such processing, the entities with whom their personal data will be shared, and the duration for which their personal data will be stored or, if that is not feasible, the criteria used to determine that period[88]. As a result, obliged entities, among them the financial institutions, will need to furnish their clients with this required information. It is possible that the exercise of the right provided for by GDPR articles 13 and 14 could potentially impair attempts, for instance by a financial institution, to combat the use of illicit funds. Informing individuals of the particulars of the data that is being held and/or collected could have the unintended consequence of alerting an individual to the nature of an institution's investigation. However, GDPR article 23(1) permits restrictions on the right to be informed in

---

[86] Under GDPR Article 49(1)(d), it is possible to transfer personal data to another country if it is necessary for *important reasons of public interest*. It is not clear whether this provision can be used to justify the transfer of personal data for the purpose of combating money laundering and terrorist financing. According to Article 49(4), the public interest must be recognized by the laws of the Member State in question in order to be considered valid, ibid Cooley

[87] GDPR article 44 where the general principle of data transfer to third countries and international organizations is provided. The specific circumstances and requirements are provided under articles 45-50

[88] In accordance with the right to be informed, see sub-chapters 1.2.3. and 1.3.1.C. of the present dissertation

certain circumstances, including where a restriction is a necessary and proportionate measure to safeguard the prevention, investigation, detection, or prosecution of criminal offenses.[89]

Another scenario of potential conflict is related to another right provided under the GDPR for data subjects. Specifically, the Regulation grants individuals the right to object to the processing of their personal data in certain circumstances, including where the processing is based on the legitimate interests of the controller or a third party, or for the purposes of direct marketing. This right could potentially hinder a financial institution's ability to process personal data for the purpose of detecting illicit financial actions, as the institution may rely on the processing of personal data as a necessary and proportionate measure to achieve this objective. The GDPR requires companies and organizations to demonstrate that they have a compelling legitimate interest in the processing of personal data that overrides the individuals' rights and freedoms, or that the processing is necessary for the performance of a contract or the exercise of a legal claim. In the case of a financial institution seeking to process personal data for the purpose of detecting money laundering and terrorist financing, they must demonstrate such a compelling legitimate interest or necessity. As a result, the right to object granted by the GDPR could potentially hinder a financial institution's ability to effectively fulfill its obligations under the AMLD.

Furthermore, pursuant to the GDPR, individuals possess the right to the safeguarding of their personal data, which encompasses any information that could be utilized to identify them. This includes information concerning their economic standing, such as details of their ownership of a company. The GDPR stipulates that any processing of personal data must be performed in conformity with the principles of data protection by design and by default[90], and that individuals must be informed about the collection and use their personal data[91].On the other hand, the AMLD aims to inhibit money laundering and terrorist financing through the enhancement of transparency in financial transactions. One method it employs to achieve this is by mandating the registration of information regarding the beneficial owners of

[89] Ibid Cooley - Legal insight for market innovators

[90] Under GDPR article 25, see sub-chapter 1.3.1.E. about the data protection by design and by default of the present dissertation

[91] Under GDPR article 13, see sub-chapter 1.2.1. of the present dissertation

companies in national transparency registers and their subsequent public accessibility. This enables authorities and members of the public to discern the individuals behind a company and potentially detect any suspicious activity[92]. However, the requirement for publicly accessible registers of beneficial owners is incompatible with the GDPR's protection of personal data. In a recent judgement, regarding the joined cases C-37/20 and C-601/20[93], the European Court of Justice (ECJ) ruled that the provision in the AMLD requiring the public accessibility of information concerning beneficial owners constituted a *serious interference* with individuals' fundamental rights to respect for private life and the protection of personal data, as protected by Articles 7 and 8 of the EU Charter of Fundamental Rights. The ECJ found that the legal safeguards in the AMLD for the protection of personal data from abuse were inadequate and therefore declared the provision null and void. As a result, national transparency registers in the EU may need to review and potentially restrict access to their registers. The ruling of the ECJ sets a precedent that protection of personal data is a fundamental right and that legislation that does not adequately safeguard personal data from abuse is incompatible with EU law.

3.2. Consequences of GDPR and AMLD non-compliance

Financial institutions, not only those operating within the EU, but those operating in third countries that have clients within the EU[94], are exposed to substantial fines for failing to comply with the provisions of the GDPR and the AMLD. Article 83 of the GDPR sets out the general conditions for imposing administrative fines for infringements of the former. The article states that administrative fines should be effective, proportionate, and dissuasive, and should be imposed in addition to or instead of other measures in certain circumstances. The amount of the fine should be based on the nature, gravity, and duration of the infringement, the character of

---

[92] AMLD 30(5)(c) according to which *Member States shall ensure that the information on the beneficial ownership is accessible in all cases to… any person or organization that can demonstrate a legitimate interest*

[93] European Court of Justice, Cases C-37/20 and C-601/20, WM/Sovim SA vs Luxembourg Business Registers, ECLI:EU:C:2022:912

[94] According to the territorial scope of application of the GDPR, as highlighted above in the 1.3. chapter of this dissertation. It should be noted that the AMLD4 scope of application is not that wide since it applies to all member states of the EU, and sets out rules and standards that financial institutions and other obliged entities within the EU in accordance with article 2.

the infringement (intentional or negligent), the level of responsibility of the controller or processor, any relevant previous infringements, and any other aggravating or mitigating factors. The GDPR specifies maximum fines for different types of infringements, ranging from EUR 10,000,000 or 2% of the total worldwide annual turnover (for the gravest infringements) to EUR 10,000 (for less serious infringements) and under. Last but not least under article 83 (5)[95], companies can be fined up to 4% of their annual global turnover or €20 million (whichever is greater) for serious violations[96]. This includes any actions that result in the unauthorized processing of personal data, such as collecting or using data without the individual's consent. Financial institutions that handle large amounts of personal data, such as banks and insurance companies, are particularly at risk of non-compliance due to the sensitive nature of the data they process.

Article 59[97] of the AMLD deals with administrative sanctions and measures that may be imposed on financial institutions and other regulated entities that breach the requirements of the AMLD. The article applies to serious, repeated, or systematic breaches of certain provisions of the Directive, including customer due diligence, suspicious transaction reporting, record-keeping, and internal controls. The sanctions and measures that may be imposed include public statements identifying the person or entity responsible for the breach, orders to cease the conduct and refrain from repetition, withdrawal or suspension of authorizations, temporary bans on individuals discharging managerial responsibilities, and administrative pecuniary sanctions. For credit institutions and financial institutions, the administrative pecuniary sanctions may be up to 10% of the total annual turnover or EUR 5,000,000, whichever is higher. For natural persons, the sanctions may be up to EUR 5,000,000. Member states may also empower competent authorities to impose additional types of administrative sanctions or to impose higher administrative pecuniary sanctions.

It is also worth noting that in case of conflicts between the GDPR and the AMLD4, the EU legislator has hinted that the framework that imposes the most severe

[95] Under GDPR article 83(5)

[96] The GDPR also allows member states to impose higher fines for certain types of infringements and to impose administrative fines on public authorities and bodies, GDPR article 83(7)

[97] Under AMLD4 article 59

penalties should take precedence. This implies that in the event of any discrepancies between the GDPR and AMLD4, the provisions of the former may be deemed to supersede any conflicting provisions within the latter. However, it is important to underline that the EU regulator has not officially established a specific hierarchy of precedence between the two regulations, although the sanctions provided by both regulatory frameworks may provide insight for the resolution of any contradictions between them.

Financial institutions that fail to comply with the GDPR and AMLD risk incurring substantial fines, as highlighted above, which serve as a deterrent to encourage compliance with these important pieces of legislation. However, it is essential to note that compliance should not be driven solely by the fear of financial penalties or administrative sanctions. Financial institutions have a duty to protect their customers' data and to prevent financial crime, and non-compliance with the GDPR and AMLD can have serious consequences beyond just financial penalties.

3.3. Potential solutions for reconciling the conflicting obligations

Financial institutions face significant challenges in reconciling the conflicting obligations provided by the AMLD and the GDPR. It is worth to be noted that the EU AML framework contains specific provisions with regards to the data protection under the chapter V of the AMLD4[98] which pursue to balance the two conflicting areas, providing rules on the prohibition of disclosure of personal data, the rights of data subjects, and the responsibility of controllers and processors for the processing of personal data.

In addition to this, one potential solution for reconciling the conflicting obligations of financial institutions under the two legal instruments is to implement appropriate technical and organizational measures to protect individuals' data and rights. The GDPR requires financial institutions to ensure a level of security appropriate to the risk, and to protect the rights and interests of data subjects. These measures may include encryption, pseudonymization, access controls, and data minimization. Financial institutions may be able to use these measures to reconcile their obligations under the AMLD and the GDPR, and to ensure that they are able to meet

[98] AMLD4 CHAPTER V Data Protection, Record-Retention and Statistical Data, articles 40-44

their obligations under both frameworks while minimizing the risk of non-compliance.

Last but not least the guidance from the relevant authorities and regulatory bodies, such as the European Banking Authority (EBA) or the European Data Protection Supervisor (EDPS) is of utmost importance. The complexity of both the regulatory schemes should be taken into consideration by the respective regulatory authorities when formulating standards and guidelines. It is not uncommon for such guidance to specifically address the relationship between the two frameworks and provide insight on how financial institutions can reconcile them in a consistent and effective manner.

Overall, the implementation of data protection in AML compliance is in its infancy and there is a lack of understanding and cooperation between the privacy and AML sectors. There is a need for the combined efforts of lawmakers, regulatory authorities, and the financial services industry to address this issue and find a solution that balances the need for data protection with the need for effective AML measures[99].

4. A BRIEF OVERVIEW OF THE US DATA PROTECTION AND ANTI-MONEY LAUNDERING REGIMES

4.1. US Data Protection regime

The data protection regime of the United States is a complex system that involves a variety of federal and state laws, as well as industry regulations and self-regulatory measures[100]. The regime's overarching goal is to protect individuals' personal information and privacy while also allowing for the responsible collection, use, and sharing of data by organizations.

---

[99] Dr. Michelle Frasher, *Multinational banking and conflicts among US-EU AML-CFT Compliance & Privacy Law: operational & political views in context* [2016], SWIFT INSTITUTE WORKING PAPER NO. 2014-008 49

[100] Jean Slemmons Stratford & Juri Stratford, *Data Protection and Privacy in the United States and Europe* [1998], IASSIST Quarterly https://iassistquarterly.com/public/pdfs/iqvol223stratford.pdf accessed on 5 January 2023

The Privacy Act of 1974[101] and the Computer Matching and Privacy Protection Act[102] play significant roles in the US data protection regime. The Privacy Act of 1974 is a federal law that establishes a set of fair information practices that are designed to balance the government's need to collect and use personal information with the privacy rights of individuals. The Act applies particularly to all federal agencies and sets out specific requirements for the collection, use, and disclosure of personal information by the government.

The Computer Matching and Privacy Protection Act, also known as the *Computer Matching Act*, is a federal law that regulates the use of computer matching by federal agencies. Computer matching involves the comparison of personal information from two or more databases, often with the goal of identifying discrepancies or errors. The Act sets out specific requirements for the use of computer matching, including the need for written agreements between agencies, notice to individuals whose information is being matched, and the opportunity for individuals to contest the accuracy of the information.

In addition to the above-mentioned legal instruments there are others that regulate specific categories of data such as Children's Online Privacy Protection Act (COPPA)[103] which provide rules for the collection of personal information from children under the age of 13[104], and the Health Insurance Portability and

[101] It was codified at 5 U.S.C. § 552a (2018), which is the section of the United States Code where it can be found. Privacy Act of 1974, 5 U.S.C. § 552a [1974], https://www.justice.gov/archives/opcl/page/file/844481/download

[102] The Computer Matching and Privacy Protection Act of 1988, also known as Pub. L. 100-503, modifies the Privacy Act of 1974. It lays out additional regulations for agencies when it comes to the use of personal information in computer matching programs, including requiring notifications, consent, data precision, data protection and remedies. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 [1988] https://www.congress.gov/bill/100th-congress/senate-bill/496/text

[103] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506 [1998] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

[104] The Children's Online Privacy Protection Act (COPPA) is applicable to operators of commercial websites and online services, including mobile apps, such as those operated by some financial institutions, if they are directed to children under the age of 13, or if they have actual knowledge that they are collecting personal information from children under the age of 13.

Accountability Act (HIPAA)[105], which sets standards for the protection of personal health information.

Except from the federal laws, there is also a number of state laws that regulate data protection, including the California Consumer Privacy Act (CCPA)[106] and the New York SHIELD Act[107]. These state laws generally provide individuals with the right to access, delete, and opt-out of the sale of their personal information.

Another significant piece of legislation that applies specifically to the financial institutions with regards to data privacy policies is the Gramm-Leach-Bliley Act (GLBA)[108], a federal law applicable to banks, credit unions, securities firms, and insurance companies. The GLBA has two main components: the Financial Privacy Rule and the Safeguards Rule. The Financial Privacy Rule establishes requirements for financial institutions to provide notice to their customers about their privacy policies and practices, as well as to obtain customers' opt-in or opt-out consent for certain sharing of their nonpublic personal information (NPI). The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the confidentiality, integrity, and availability of customers' NPI. In summary, the GLBA imposes on the financial institutions the obligation to protect the privacy of their customers' NPI by implementing and maintaining a comprehensive information security program.

The US and EU data protection regimes are similar in that they both aim to protect individuals' personal information while also allowing for the responsible collection, use, and sharing of data by organizations. Both regimes also provide individuals with certain rights in relation to their personal information, such as the right to access and request the deletion of their personal data. Overall, while the US and EU data protection regimes share some similarities, they also have some significant differences in terms of the level of legal protection afforded to personal

---

[105] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [1996] https://www.congress.gov/bill/104th-congress/house-bill/3103/text

[106] California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.199 [2018] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[107] Stop Hacks and Improve Electronic Data Security (SHIELD) Act, N.Y. Gen. Bus. Law § 899-aa [2019] https://www.nysenate.gov/legislation/bills/2019/a5635/amendment/b

[108] Gramm-Leach-Bliley Act. [1999]. Public Law 106-102, https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

information[109] and their approach of the collection and use of personal data for commercial purposes.[110]

Overall, the data protection regime in the US is multifaceted and constantly evolving, with a variety of laws and regulations in place to protect individuals' personal information and privacy. While there is still room for improvement, in comparison with the EU regime[111], the US has established a robust framework for data protection that helps to safeguard the data processing.

4.2. US Anti-Money Laundering regime

The US AML regime aims to disrupt money laundering activities by imposing obligations on financial institutions and other regulated entities to report suspicious activities, maintain records of transactions, and implement internal controls to prevent money laundering. It is unsurprising that the United States is a leader in the global effort to combat money laundering, given the large volume of illicit funds that pass through its banking system[112].

The US AML regime is composed of federal laws and regulations, as well as guidance from government agencies and self-regulatory organizations. The most important federal laws include the Bank Secrecy Act (BSA) of 1970[113], the Money Laundering Control Act (MLCA) of 1986[114], and the USA PATRIOT Act of 2001[115]. The BSA

---

[109] The EU has a comprehensive data protection framework, the GDPR which establishes a set of strict rules for the collection, use, and sharing of personal data. In contrast, the US does not have a single, comprehensive federal data protection law, as mentioned above and the level of legal protection afforded to personal information varies depending on the sector and the state in which the data is collected.

[110] The GDPR sets out strict rules for the use of personal data for marketing and advertising, and requires companies to obtain explicit consent before using personal data for these purposes, under article 7. In the US, the level of protection afforded to personal data for commercial purposes is generally weaker, and companies are often able to use personal data for marketing and advertising without obtaining explicit consent.

[111] Davide Szép, *Anti-Money Laundering and Privacy: Are They Interrelated or in Conflict? A Comparison Between the U.S. and the E.U* [2017], NYSBA NY Business Law Journal Vol. 21 No. 2 37

[112] Nicholas Ryder, *Money Laundering - An Endless Cycle? A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada* [2012], Routledge, London 5

[113] Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 [1970] https://www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf#page=14

[114] Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207 [1986] https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg3207.pdf

requires financial institutions to maintain records of transactions and report suspicious activity, while the MLCA criminalizes money laundering. The USA PATRIOT Act expands the scope of the BSA and MLCA and enhances the powers of law enforcement agencies to combat money laundering and terrorism financing.

In addition to these federal laws, the US AML regime includes regulations from various government agencies, such as the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC). FinCEN is a bureau of the US Department of the Treasury that is responsible for implementing and enforcing the BSA. OFAC is also a part of the Treasury Department and is responsible for administering and enforcing economic and trade sanctions against foreign countries, terrorists, and other designated individuals and entities.

The US AML regime also relies on self-regulatory organizations, such as the Financial Industry Regulatory Authority (FINRA) and the American Bankers Association (ABA), to provide guidance and best practices to financial institutions and other regulated entities. FINRA is a private organization that regulates the securities industry, while the ABA is a trade association for the banking industry.

Both the US and EU AML regimes have been effective in detecting and disrupting money laundering activities. However, they have main differences among which e.g. the scope of the regulations. The US AML regime applies to a wide range of financial institutions and other regulated entities, including banks, money service businesses, securities broker-dealers, and casinos, among others[116]. In contrast, the EU AMLD applies to a more limited set of financial institutions and other regulated entities, including banks, credit institutions, money remitters, and insurance companies.

It is worthy of mention that the EU AMLD, compared to the US AML framework has garnered criticism due to its implementation by member states, as certain countries have been slow to transpose the Directives into national law and have not fully implemented its provisions.

In the US, there may be potential conflicts between the requirements of the AML regime and data protection rules, likewise within EU, as described in the previous

---

[115] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

[116] For example, BSA

chapters[117]. To address this potential conflict, financial institutions and other regulated entities may need to implement policies and procedures that ensure compliance with both AML and data protection requirements. This may involve implementing appropriate safeguards to protect personal data, such as encryption and secure storage, and obtaining the necessary consent or legal basis for the collection, use, and disclosure of personal data.

To summarize the information discussed in the previous two sub-chapters, which pertains to the regulatory frameworks in place in the EU and US, the potential conflicts between their provisions, and the resolutions from each jurisdiction, the following key points will be highlighted:

The EU and US have different regulatory frameworks for data privacy and anti-money laundering; the EU's GDPR is considered to be more comprehensive in terms of data protection compared to the US's framework. The EU regulators' emphasis on privacy as a fundamental human right and its inclusion in the constitutions of member states[118], in contrast to the US where privacy rights are not explicitly protected by the constitution, reflects this difference. The EU's AMLD4 also incorporates data protection considerations in compliance policies and procedures, further emphasizing the EU's commitment to privacy.

Conversely the US AML regime does not necessitate the incorporation of privacy considerations in compliance policies and procedures[119]. The US's approach is based on a risk-based approach which involves assessing the risks associated with potential money laundering and terrorist financing activities, and implementing measures that are proportional with those risks. This approach allows financial institutions and other regulated entities to focus their resources on the areas of greatest risk, rather than implementing a one-size-fits-all approach. However, this approach is in contrast to the EU data protection framework, which is founded on a rule-based approach and allows for limited exemptions[120].

---

[117] See chapter 3.1. of the present dissertation regarding the scenarios of the potential conflicts between the two legal schemes

[118] Ibid

[119] Davide Szép, 35

[120] Ibid 35

The contrasting perspectives on data privacy and anti-money laundering between the EU and US are rooted in cultural and societal differences between the two regions. As a result, there is a lack of legal guidance on how to reconcile these discrepancies, particularly for multinational financial institutions. The author contends that the EU's commitment to personal data safeguarding may serve as a resolution to potential conflicts between the two frameworks, in contrast to the US regime which places more emphasis on the AML rules. Nevertheless, it is important to acknowledge that the US system's strict focus on risk-based approaches renders it robust, and potentially the most effective globally.[121]

5. CONCLUSIONS

The Anti-Money Laundering Directives (2015/849 & 2018/843) and the General Data Protection Regulation (2016/679) both aim to protect the interests of individuals and society, but they do so in different ways. The AML Directives are designed to prevent money laundering and terrorist financing, while the GDPR focuses on protecting the personal data of individuals. As a result, specifically regarding data processing, there is potential for conflict between these two sets of regulations. This contradiction can be a complex issue, as examined in the chapters of the present dissertation. It is important for financial institutions to carefully consider and balance their obligations under both sets of regulations in order to ensure compliance and avoid any negative consequences.

The main objective of this dissertation was to shed light on the interplay between the GDPR and the AMLDs, and to provide insights into the ways in which financial institutions can navigate and comply with the requirements of both the legal instruments while also protecting their customers' privacy and personal data. In the author's view, while there may be some tensions between GDPR and AMLD provisions, the measures put in place to address and mitigate these conflicts and to prevent confusion for financial institutions have clearly been taken into consideration by the European legislator, as evidenced by the inclusion of data protection provisions within the AMLD framework.

[121] Ibid 38

To conclude this dissertation, the following comment from the author is offered: It is undeniable that the rapid pace of technological advancement in recent years has brought about numerous new opportunities and innovations in the financial sector. At the same time, however, it has also created new challenges and risks, particularly in the areas of money laundering and terrorism financing. Criminals and terrorists are constantly seeking to exploit new technologies and techniques to carry out their illicit activities, and financial institutions and regulators must be prepared to adapt and respond to these evolving threats. In addition to these security concerns, there is also the need to protect personal data as financial institutions handle sensitive customer information on a regular basis and it is crucial that they stay up to date with the latest requirements and best practices for data protection.

In order to effectively combat financial crimes, while also complying with data protection needs, it is essential that the legal frameworks governing the aforementioned areas are regularly updated and revised to reflect the latest developments in technology and financial services. This is especially important given the transnational nature of these crimes and the need for cooperation and coordination among different countries and jurisdictions. By staying up to date with the latest trends and best practices, financial institutions can better protect themselves, their customers, and their sensitive data from illicit types of activities and help to ensure financial system’s integrity.

6. BIBLIOGRAPHY

Article 29 Data Protection Working Party, EU General Data Protection Regulation – General Information Document [2016], available at: https://www.appaforum.org/wp-content

Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 [1970] available at: https://www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf#page=14

Blackmer W. Scott, GDPR: Getting Ready for the New EU General Data Protection Regulation [2016], Information Law Group, available at: https://web.archive.org/web/20180514111300/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.199 [2018] available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Charter of Fundamental Rights of the European Union, EU Charter [2000] OJ C 326

Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506 [1998], available at: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Comply Advantage 6AMLD: 6th Money Laundering Directive, https://complyadvantage.com/insights/6th-money-laundering-directive-6amld/

Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 [1988] available at: https://www.congress.gov/bill/100th-congress/senate-bill/496/text

Consumer Privacy World, Overview of Privacy & Data Protection Laws: Europe, available at: https://www.consumerprivacyworld.com/privacy-europe/

Cooley - Legal insight for market innovators, GDPR and AML – a perfect pair? [2018] available at: https://cdp.cooley.com/gdpr-and-aml-a-perfect-pair/

Cotter Daniel, USA: Anti-money laundering and bank secrecy in relation to privacy [2019], https://howardandhoward.com/user_area/pdf

Council of Bars and Law Societies of Europe, Efficiency in anti-money laundering regulation - The path to combating the laundering of proceeds of crime effectively [2020], The voice of European Lawyers, available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/ANTI_MONEY_LAUNDERING/AML_Position_papers/EN_AML_20200626_Efficiency-in-anti-money-laundering-regulation-The-path-to-combatting-the-laundering-of-proceeds-of-crime-effectively.pdf

Court of Justice of the European Union, Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] OJ C212/4

Court of Justice of the European Union, Cases C-37/20 and C-601/20, WM/Sovim SA vs Luxembourg Business Registers, Court of Justice ECLI:EU:C:2022:912

Data Protection Commission, Guidance note: Legal Bases for Processing Personal Data [2019], available at: https://www.dataprotection.ie/sites/default/files/

De Groot Juliana, What Is Data Encryption? Definition, Best Practices & More [2015], available at: https://digitalguardian.com/blog/what-data-encryption

Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014], OJ L 173/349

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market [2007], OJ L 319

Directive (EC) 91/308 of the Council 10 June 1991 of on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77

Directive (EC) 01/97 of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering [2001] OJ L344/76

Directive (EC) 2005/60 of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [2005] OJ L309/15

Directive (EC) 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 L141/73

Directive (EC) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 L156/43

European Court of Auditors, The EU's anti-money laundering policy in the banking sector [2020], available at: https://www.eca.europa.eu/lists/ecadocuments.pdf

European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects [2019], available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

European Data Protection Board, Guidelines 3/2018 on territorial scope of the GDPR (Article 3) [2020], available at: https://edpb.europa.eu/sites/default/files

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default [2020], available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904.pdf

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law [2018] available at: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

Frasher Michelle, Multinational banking and conflicts among US-EU AML-CFT Compliance & Privacy Law: operational & political views in context [2016], SWIFT INSTITUTE WORKING PAPER NO. 2014-008 49

Gál István László, The 2018/843 EU Directive on the prevention of money laundering and terrorist financing and its correlation to the criminal law prevention of the stock markets [2019] available at http://real.mtak.hu/100887/

Glynn Laura, KYC vs Data Protection – The next compliance hurdle [2016] Fenergo 11

Gramm-Leach-Bliley Act. [1999]. Public Law 106-102, https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [1996] available at: https://www.congress.gov/bill/104th-congress/house-bill/3103/text

Kot Marek, Impact of the 5th Anti-Money Laundering Directive on EU's financial market, Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges, 11641

Lomas Natasha, e-Privacy: An overview of Europe's other big privacy rule change [2018], Tech Crunch, available at: https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/

Milaj Jonida - Kaiser Carolin, Retention of data in the new Anti-money Laundering Directive — 'need to know' versus 'nice to know [2017] 7(2) International Data Privacy Law

Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207 [1986] available at: https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg3207.pdf

Privacy Act of 1974, 5 U.S.C. § 552a [1974] available at: https://www.justice.gov/archives/opcl/page/file/844481/download

Protecto, Data Minimization: Checklist, strategies and steps, available at: https://www.protecto.ai/wp-content/uploads/2022/01/Data-Minimization-Strategies-and-Steps-Protecto.pdf

Reese Bernadine, GDPR and EU AML Directives – A Regulatory Tug-of-War? [2018], Protiviti Global Business Consulting, available at: https://blog.protiviti.com/2018/05/24/gdpr-eu-aml-directives-regulatory-tug-war/

Regulation (EC) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119

Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories [2012], OJ L 201

Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies [2009], OJ L 302

Robinson Neil, Graux Hans, Botterman Maarten, Valeri Lorenzo, Review of the European Data Protection Directive [2009], Rand Corporation, available at: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dpdirective.pdf

Ryder Nicholas, Money Laundering - An Endless Cycle? A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada [2012], Routledge, London 5

Selzer Annika, Woods Daniel and Böhme Rainer, Practitioners' Corner - An Economic Analysis of Appropriateness under Article 32 GDPR [2021], European Data Protection Law Review, Volume 7, Issue 3

Slemmons Stratford Jean & Stratford Juri, Data Protection and Privacy in the United States and Europe [1998], IASSIST Quarterly https://iassistquarterly.com/public/pdfs/iqvol223stratford.pdf

Stop Hacks and Improve Electronic Data Security (SHIELD) Act, N.Y. Gen. Bus. Law § 899-aa [2019] available at: https://www.nysenate.gov/legislation/bills/2019/a5635/amendment/b

Szép Davide, Anti-Money Laundering and Privacy: Are They Interrelated or in Conflict? A Comparison Between the U.S. and the E.U [2017], NYSBA NY Business Law Journal Vol. 21 No. 2 37

Tikkinen-Piri Christina, Rohunen Anna, Markkula Jouni, EU General Data Protection Regulation: Changes and implications for personal data collecting companies [2017], Computer Law & Security Review: The International Journal of Technology Law and Practice, doi: 10.1016/j.clsr.2017.05.015

USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf