J U R I D I C U M

Processing Financial Crime Data under the GDPR
in the light of the 5th Anti-Money Laundering Directive

Christa Savia

VT 2019

RV600G Rättsvetenskaplig kandidatkurs med examensarbete (C-uppsats), 15 högskolepoäng

Examinator: Katalin Capannini-Kelemen
Handledare: Cristina Trenta

Summary

The study explains how financial crime data can be legally processed under the General Data Protection Regulation, especially regarding the 5th Anti-Money Laundering Directive. Financial crimes are a growing problem which requires effective processing for preventing crimes. To prevent financial crimes, financial institutions are obligated to process large amounts of data on a daily basis. The development of internet services, technology and globalisation, have affected the financial crimes which have become more common and harder to prevent. To prevent crimes on internet has led to process and collect more and more data for different databases. The increasing amount of data processing requested the need for an updated version of data protection legislation which would harmonise the process between the Member States of the EU. This led to formulating of the General Data Protection Regulation, which was accepted in 2016 and applied to the EU Member States national laws. The General Data Protection Regulation is described as one of the most efficient data protection legislation protecting individuals' rights considering the processing and collecting the data. The new legislation regarding data process was well needed since collecting personal data has been more common in daily practice.

In addition, the study analyses the balance between the General Data Protection Regulation and the 5th Anti-Money Laundering Directive. The analysis is made in light of the relationship between Know Your Customer principle regarding to the data protection, and how the balance of interest is applied in the financial sector. The study examines how financial institutions are able to apply the new Regulation without losing the effectiveness of preventing financial crimes, for instance, in relation to money laundering. For preventing financial crimes, the collected data can be sensitive, which makes the data protection of individuals extremely important. This has led to complexity between financial institutions and the General Data Protection Regulation.

Keywords: Financial crime data, General Data Protection Regulation, Anti-Money Laundering, Data, EU Law, Data Processing

Abbreviations

4th AML	4th Anti-Money Laundering Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
5th AML	5th Anti-Money Laundering Directive 2018/843 on the prevention of the use of financial system for the purposes of money laundering or terrorist financing
The Charter	The Charter on Fundamental Rights of the European Union
CJEU	The Court of Justice of the European Union
DPA	Data Protection Authority
The Data Protection Directive	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
ECHR	The European Convention on Human Rights
EDPS	The European Data Protection Supervisor
EEA	European Economic Area
EU	The European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GDPR	Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
IMF	International Monetary Fund
KYC	Know Your Customer
TEU	The Treaty of the European Union
TFEU	The Treaty on the Functioning of the European Union
VPN	Virtual Private Network

Table of Contents

1. Introduction

1.1 Background

Nowadays, everything is on the internet. While accessing new websites, we have learnt to accept cookies automatically. Internet collects data, our computers and mobiles collect data, and we even receive advertisements and emails based on our web searches. We give our personal information to different webpages without questioning it. Heretofore we had to visit banks and offices to receive information about our accounts or perform simple tasks. Today, because of mobile identifier applications, we do not have to visit offices to receive the information. By giving a fingerprint or a code via one the applications, we reach all the data needed.

However, is there a downside to collecting and receiving all this information so easily? Wouldn't it be great that state authorities and bank offices can collect the data? Being able to save and share data gives authorities a better view of their customer base. It also gives possibilities to have different types of registrations, which can be useful *inter alia* to financial authorities. Since we have everything on the internet, it has tempted criminals to develop different types of criminal actions, including but not limited to money laundering, and identity crimes. After the development of the internet, criminals can use anonymous accounts, a virtual private network (VPN)[1] and other hidden networks to process money through internet banks, even abroad without leaving a record of the process or source of money. Without a record of the process or source of money, the risk of abuse increases.

There is a certain risk to deal with financial acts, and many financial institutions use credit scores to minimise risk factors. Therefore, it would be a great thing if financial authorities could co-operate with each other by collecting information about their customers, and they would be able to access a database to protect financial security. By having a shared database, the possibility of preventing crimes would arise, and financial authorities would not need to take such a huge risk while accessing a new business relation.[2]

However, having a database creates a problem with saving individuals' data. The amount of data processing has notably increased in recent years, which has not been foreseeable. For both customers and authorities, it is hard to tell which information is necessary to collect and which information can be unnecessary or even harmful. There is a huge chance that we are not even sure about the information we give, or the information collected from us. There have not been clear regulations, guidelines or legislation on how to process personal data by the international law. States have applied national legislation while collecting and using personal data, which creates international conflicts while conducting this type of information.

In 2012 the European Commission presented a proposal to a new data protection regulation.[3] The proposition aimed to create updated data protection regulation, which would be accurate to

[1] VPN is a technical term used in the internet, when the user wants to access to public network as a private use, which gives users a possibility to access the internet anonymously and secure their identity. The VPN can be used to block data collecting or users can create own hidden network without leaving track.
[2] Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2018) The FATF Recommendations 9.
[3] Presidency of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach' (2012) Council of the European Union, COM/2012/011.

the current situation. After four years of work, the General Data Protection Regulation (GDPR) with 99 articles was accepted on 14th of April 2016, entered into force after the twentieth day of its publication on Official Journal of the European Union and implemented on 25th of May 2018 to all European Union (EU) Member States.[4]

The GDPR is the latest update in European legislation protecting data, affecting in the EU and European Economic Area (EEA). The GDPR gives stricter rules on how to process personal data and how to protect individuals' rights while processing their personal data. However, GDPR has a couple of exceptions which allows the GDPR to process financial crime data with the help of *inter alia* the 5th Anti Money Laundering Directive (5th AML)[5].

For the financial sector, effective data management is an essential factor. Financial institutions are used to process large amounts of data in regard to principles and obligations the financial sector has, for instance, *Know Your Customer* principle. Since the GDPR, financial institutions had to prepare themselves for new changes considering data processing. Financial institutions are often requested to apply different financial regulations and co-operate with different financial authorities. This raises the complexity of legal data processing and the collected information. The GDPR aims to minimise the amount of processed data, which creates a complexity between the Regulation and financial institutions.[6]

1.2 Aim and Research Questions

This study aims to analyse and investigate the EU law issues regarding processing financial crime data under the General Data Protection Regulation. The financial sector is developing at the time, as is data protection. Financial crimes are a big threat to the society, which makes processing the financial crime data by the proper way to be very important. Furthermore, the study aims to investigate the legal obligations the financial institutions have, while processing data on the EU law perspective. In addition, the study analysed the relationship between GDPR and 5th AML under financial crime data.

After the GDPR, there have been major changes in how personal data can be collected and used; therefore, the study focuses on three main areas. Firstly, the study examines the balance between collecting financial crime data and protection of personal data under the GDPR. By referring to term *financial crime,* the study concentrates on analysing it on money laundering's aspect. The GDPR gives a whole new legislation on how to process and protect personal data, which have to be considered even in the financial sector.

Secondly, the study investigates the ruling between the GDPR and Anti-Money Laundering Directives, concentrating on the 5th AML and Know Your Customer (KYC) principle. The 5th AML gives basic guidance on how to prevent money laundering and how to protect financial institutions from financial crimes. Anti-Money Laundering Directives include guidance regarding how financial crime data should be processed. Hence, the study analyses how the GDPR is affecting the 5th AML and what is the relationship between them.

---

[4] 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 (Data Protection Directive) [2016] OJ L119/1.

[5] 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 article 1.

[6] Olly Jackson, 'Many small firms are still unprepared for GDPR' (2018) International Financial Law Review.

Lastly, the study analyses how 5th AML and the GDPR are affecting the financial security by examining the balancing of interest while processing the data, and risk-based analysis on the financial sector. These research questions are analysed through the study of relevant material. The study focuses on finding the relationship between the GDPR and the 5th AML in a way financial crime data can be processed legally. Furthermore, the study expects to find how the GDPR affected the financial sector and how the GDPR and Anti-Money Laundering Directives ensure financial security.

1.3 Method and Sources

As mentioned, financial institutions have had some changes after the GDPR. Processing financial crime data is an international issue which needs to be taken seriously. After the GDPR and the changes, the EU Member States have harmonised international and national laws in regard to data protection. However, there are still some problems while applying the GDPR. The study applies juridical methods and legal dogmatic methods, which are based on interpretation, systematisation and analysing of legal material. The source for the study is the existing law.[7]

Furthermore, the study is an analysis of the European Union's regulations, directives and the relationship between them. The source for the study is existing EU law, the study is made on the EU law's perspective and analyses how the laws are applied in the European Union. Therefore, the study adopts also the EU legal method.[8]

The EU is an international organisation, which includes 28 Member States.[9] EU is located in Europe, implementing laws and guidelines to its Member States. The EU has institutions which are affecting various ways to society, for instance policy-making bodies and the European Commission. The EU legislation includes treaties which are categorised as primary legislation; and regulations, directives and decisions which are concerned as secondary legislation.[10] The EU legislation is based on many different sources of law which makes it suitable for the Member States, who are applying the laws to their national legislation. The EU prevents its Member States to act independently concerning international cases and international law by harmonising the Member States' legislation.[11]

The Treaty on the Functioning of the European Union (TFEU)[12] is one of the two treaties of the EU. The other one is called Treaty on European Union (TEU)[13]. The TFEU is considered as the constitution of the EU and known as the basis of the Union law. TFEU provides ruling for secondary union legislation under articles 288-294 TFEU. According to mentioned articles,

---

[7] Maria Nääv, Mauro Zamboni, *Juridisk metodlära* (2nd edn, Studentlitteratur 2018) 21.
[8] Ibid 110.
[9] Currently the EU has 28 Member States, but after the Brexit (portmanteau; British and exit) there will remain 27 Member States. In 2016 the United Kingdom announced their withdrawal from the EU waving on article 50 of TEU. After the announcement there has been a lot of negotiation how the process will continue and how this is affecting to the other EU Member States. The United Kingdom was supposed to withdraw on 12 April 2019 but the United Kingdom requested the extension to end of the June, and until the October 2019 the United Kingdom will be the Member State of the EU.
[10] European Union 'EU Law' (*Europa EU*, 27 February 2019) <https://europa.eu/european-union/law_en> accessed on 28 March 2019.
[11] Margot Horspool, Matthew Humphreys, Michael Wells-Greco, *European Union Law* (9th edn, OPU 2015) 96.
[12] The Treaty on the Functioning of the European Union [2016] OJ C202/01 (TFEU).
[13] The Treaty on European Union [2016] OJ C202/01 (TEU).

regulations, directives and decisions are binding EU law. As mentioned in article 288 of TFEU, the regulations shall be directly applied to all Member States national legislation. Therefore, the GDPR was directly applied and did not have to be incorporated into the national legislation. However, directives have binding effect, but they leave the choice as to form and method for the Member State, mentioned in article 288 TFEU. Therefore, directives must be incorporated into the national legislation, but the Member States have a wider interpretation while adopting the directive to the national legislation, *e.g.* the 5th Anti-Money Laundering Directive. Decisions are binding for those to whom they are addressed, and therefore, decisions have more specific measures.[14]

1.4 Delimitations

The GDPR is a large topic as is financial crime data. Even though the study analyses the GDPR in the light of the 5th Anti-Money Laundering Directive, the study does not go deeply into terrorism on the financial sector. Therefore, the study concentrates to money laundering in financial crime sector and analyses the money laundering's aspect in financial crimes. Furthermore, the study discusses briefly criminal aspect and criminal law, for example, authorities' roles are mostly discussed as administrative authorities. Hence, the study limits criminal judgments to the minimum.

The study concentrates on the EU's Member States and EEA area by analysing the issue on a legal aspect. The study does not concentrate on any other methods. The study is not going to go to third-party countries or analyse GDPR on another aspect other than finance, on money laundering aspect. Also, the study aims to analyse private persons and their rights concerning financial crime data processing; the study is not going to analyse legal persons' aspect.

1.5 Outline

The first part of the study is an introduction to the topic, which includes the explanation of the background, the aim of the study, legal issue analysed in the study and the method of the study. The second part of the study introduces the theoretical part of the study by discussing data processing and the GDPR by giving a view of the Regulation and introducing the legal framework. This part also introduces the legal framework of AML and examines it with the help of the GDPR. In the third part, the study analyses and investigates financial crime data, in the view of the European Union's legislation. The analysis presents the findings of the study and concludes them.

The study concentrates to the EU legislation, especially to the GDPR and the 5th AML. The study uses relevant articles between the chapters and explains how the relevant articles are applied and used in the EU. Thus, the reader will reach relevant articles directly in the study. For receiving a deeper understanding of the study, the reader can research the GDPR and the 5th AML.

[14] Margot Horspool, Matthew Humphreys, Michael Wells-Greco, *European Union Law* (9th edn, OPU 2015) 102-104.

2. Processed Data

In this chapter, the study discussed the theoretical part of what is concerned as data, how to define personal data besides of what is financial crime data. Furthermore, the study introduces the Financial Action Task Force (FATF), their recommendations concerning financial sector and its international legislation, Data Controllers role while processing data especially in regard to financial authorities and the aim of know your customer rules.

2.1 What is considered as a Data?

Everything that can be related to identifying a person or is an identifiable in relation to individual is conducted as personal data. Also, information which is collected together and can lead to identifying a person is considered as data. Personal data does not include anonymously collected or render information, neither it does fall under the scope of the data protection. The personal data is not relatable to which technology it is used on, the data protection scope is falling in both, automated and manual process. The same rule applies to the storing rules; the data can be collected *inter alia* by video system, IT system or by paper. For the EU Member States, the accordant legislation for treating personal data is the GDPR.[15] The GDPR defines the term "personal data" under article 4 (1) as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[16]

By referring to natural persons, the article refers to a human being or an individual who also has a legal personality as article 4 (1) mentions, any information, including data where a person can be identified falls under the scope of the article. This means even non-personal information can become personal information by combining it with other information if the person can be identified from it. The article aims to protect the data process and to prevent collecting unnecessary data.[17]

The word "processing" in legal terms means an operation which is set to perform personal data, even if the process is automated. Article 4 (2) under the GDPR clarifies that any treatment of data will fall under the scope of the article, even when erasing the data.[18] The data itself is a complex term, which is especially analysed in the GDPR. Mainly, the term "data" reflects to electronically recorded information. To be concerned as personal data, the data has to include identifiable information. Identifiable information means both data where a person can be

[15] European Commission 'What is Personal Data?' *(EC Europa EU)* <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> accessed on 29 March 2019.
[16] 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 (Data Protection Directive) [2016] OJ L119/1 Article 4 (1).
[17] Marcelo Corrales, Mark Fenwick, Nikolaus Forgó, *New Technology, Big Data and the Law* (Springer 2017) 21.
[18] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 10.

directly identified or indirectly identified. This kind of information can be *inter alia* name, identification number, photographs, location data or IP-address.[19]

2.2 Financial Crime Data

Financial crime, also known as economic crime, means crime or illegal acts committed by individuals to receive a financial benefit and they often have a low risk and huge profit.[20] Financial crimes are a new type of crime concerning criminal law and were criminalised only approximately 20 years ago, on the 1990s in most countries. Financial crime in itself is a wide term, but in the everyday language, financial crimes are mostly affiliated as a money laundering or financing terrorism. The study concentrates on financial crimes from a money laundering perspective, which as a term means that someone is trying to hide the origin of the illegal money by making that money appear as legal property.[21]

Financial crime investigations and identifying illicit transactions are becoming harder and harder for law enforcement agencies. Noticing illicit financial flows would need years of training for state agencies. Thus, Anti-Money Laundering Directives have transferred the responsibility of investigating financial crimes to financial authorities. In Europe, the legislation for financial crimes is decreed on Anti-Money Laundering Directives; the current version is called the 5th AML.[22]

The general rule of storing personal data in the EU is that the data should be erased after the data is no longer relevant for the use or necessary for the purpose of processing data. However, there is an exception concerning special data retention. *Inter alia* the GDPR takes legitimate interest and legal obligation into account.[23] Reason to collect and retain the data can be, *e.g.* suspicion or connection to the crime or the data can be used in an investigation. Financial authorities are obligated to investigate and report financial crimes or if they are suspicious of a crime taking place. Financial crime data can include, *e.g.* information to prevent money laundering, persons that have committed a financial crime and persons connected to terrorist financing. Financial authorities, such as banks and business corporations, are collecting and processing this kind of information on a daily basis. A so-called background check can occur when an individual is applying for a loan from the bank, or the bank does a credit control check.[24]

[19] Ibid 11.
[20] Europol 'Economic Crime' *(Europol Europa EU)* <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime> accessed on 29 March 2019.
[21] 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://doi-org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 2nd May 2019 118.
[22] Ibid 116.
[23] 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 (Data Protection Directive) [2016] OJ L119/1 articles 6 (1) (c) and 6 (1) (f).
[24] 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://doi-org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 2nd May 2019 122.

2.2.1 The Financial Action Task Force

The Financial Action Task Force (FATF)[25] is one of the largest international financial authorities, which advices on implementing of financial legislation and operating *inter alia* on following areas: money laundering, terrorist financing and to other international financial threats. The FATF is the so-called "policy-making body", and they develope recommendations that are recognised internationally. The meaning of these recommendations is to set standards for combating against financial crimes. The FATF has 38 members at the moment; one of them is the European Commission.[26]

The FATF aims to secure countries, strengthen countries legislation and knowledge in risk situations and where the rights could be enhanced. The FATF fights against financial criminality and help their Member States to fight against financial criminality by helping them implement their recommendations. The recommendations are reviewed with private sectors, civil societies and with other interested parties who are willing to secure the financial sector.[27] The FATF has received authority and responsibility to examine money laundering on various levels, reviewing how the issues have been solved on both national and international level and giving suggestions what could be done for preventing increases of similar issues. The FATF has followed current issues of the world and included them to their internationally recognised recommendations.[28]

However, the FATF has received some criticism. The FATF is not an UN-body, nor has its legitimacy been fully established. Being a Member State of the FATF is voluntary, and it is authorities own choice to decide how much weight and impact the FATF recommendations have. Even though being a Member State is not mandatory and the choice is left up to countries, most of the EU Member States have decided to join the FATF since its recommendations are similar of the European financial integration. The FATF neither has an accountability mechanism which could help countries to apply its decisions, or the FATF could report its oversights. The problem area concerning the FATF is that it is not accepted universally although they are internationally recognised, *inter alia* India has not accepted the FATF recommendations.[29]

By being criticised and officially being more a political ministry than having universally accepted legitimacy, the FATF has created a significant impact on the financial industry. Because of the FATF, the financial institutions are monitored more closely, the International Monetary Fund (IMF) has a stronger impact on credit conditions, and individuals use of credit cards (*e.g.* sending money abroad) are investigated due to money laundering.[30] The FATF has helped to develop the international co-operation between financial institutions and the secure international business affairs by harmonising the investigation process and the credit conditions. The reforms and recommendations have helped to decrease illicit activity, yet the need for universal acceptation and standards are still needed to reach the maximum balance and

[25] The Financial Action Task Force, http://www.fatf-gafi.org/home/. The Financial Action Task Force was founded on 1989 by group called "Group of Seven".
[26] The Financial Action Task Force, 'Who we are' *(FATF GAFI)* <http://www.fatf-gafi.org/about/> accessed on 29 March 2019.
[27] The Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2018) The FATF Recommendations.
[28] Usman W Chohan, 'The FATF in the Global Financial Architecture: Challenges and Implications' (2019) Social Science Research Network 5.
[29] Ibid 8.
[30] Ibid 12.

security between countries. Therefore, the FATF hopefully receives universally accepted legitimacy by continuing work against illicit financial activity.[31]

2.2.2 Data controllers

Data controller is an often used term on a financial sector concerning data processing. The term "data controller" means an individual who itself or with others decides and examines the purposes of the data process, if the purpose behind the process is legal and in accordance with the Union or the Member States' legislation. According to the GDPR, a data controller can be a natural person, a legal person or a person having status as a public authority.[32] If the data controller is part of the EU Member States, or the data affects one of the Member States, the GDPR applies while applying the data, and the regulation binds the controllers. Since the data controllers are responsible for the data, they have to record the process of how the data is collected and used. Companies have data processors who are only processing the data on behalf of the controller. The difference between the controller and the processor is not huge, but the controller has more responsibilities and is more restricted by the legislation.[33]

After the GDPR was enacted and entered into force, there were huge changes in the industry. The collected data needs to be processed, analysed and saved for the customers, according to the rules of the regulation. Hence, customers can know how their data is used. Many financial institutions have to manage huge amounts of data per day, for instance when verifying business unit, while continuing monitoring and while analysing and reporting the behaviour of the customer.[34]

2.3 Know Your Customer

Money laundering is a serious crime and must be concerned as a threat to the financial sector and economical well-being of society. In recent years countries have started to implement laws against money laundering, and there is no denying that financial institutions have created preventative strategies, one of them is called "Know Your Customer" principle.[35] Know Your Customer (KYC) is an often used term in the business and financial world. Financial authorities are in need to collect customers' data and to have an adequate relationship between the authority and the customers for preventing crimes. Processing data is mandatory for the financial institutions, *e.g.* banks, to have a full understanding of the risks the customer can pose to the bank and society. KYC is a process that financial institutions are taking to verify their customers and to minimise potential risks while entering into a business relationship. The KYC aims to prevent financial institutions from being used in illegal financial activities.[36] In the EU, KYC

---

[31] Judith E Tyson, 'International financial centres and development finance' (2019) ODI Report 8.
[32] 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 (Data Protection Directive) [2016] OJ L119/1 article 4 (7).
[33] Francoise Gilbert 'EU General Data Protection Regulation: What impact for Businesses Established Outside the European Union' (2016) 19 (11) Journal of Internet Law 1-7 <https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=115322774&site=ehost-live> accessed on 30 March 2019.
[34] 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 (Data Protection Directive) [2016] OJ L119/1 recital (10)-(11).
[35] Renny See Benedictus, Miru Ahmadi, Hasbir Muhadar, Paserangi, 'Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes' (2019) JL Pol'y & Globalization, 81-101 101.
[36] Dennis Cox, *Handbook of Anti-Money Laundering* (John Wiley & Sons 2014) 169.

rules are presented in the Anti-Money Laundering directives, especially in the 5th Anti-Money Laundering Directive is focusing on preventing money laundering and financing terrorism. For KYC to be successful, financial institutions need to process a lot of data to understand the customer's actions and activity. Without having the necessary information, it is not recommended to co-operate with the customer concerning the risks.[37]

Furthermore, the KYC principle is included on the FATF recommendations, which suggest recording the data for both the analysis of preventing money laundering and for investigations. These recommendations are called FATF 40 recommendations and published annually. The recommendations are often written with broad interpretation giving the possibility for the Member States to interpret recommendations into their national legislation. The FATF aims to create widely recognised standards for KYC principle while trying to minimise the use of resources of financial institutions.[38] Recently it has been more and more common that banking industry is required to apply KYC principle to be able to monitor customer accounts and record the source of the data to know where the data is collected and what data is collected. Following the KYC principle, the banking industry can identify customer and customers behaviour, which helps to identify possible crimes and minimises the legal risks. The KYC principle is one of the most effective efforts on the financial sector to prevent money laundering, whether it is applied directly or indirectly to perpetrators of crime.[39]

The problem of the KYC principle is the lack of public knowledge concerning banking and financial services. The lack of understanding of the importance of collecting the data is one of the biggest obstacles the banking industry has faced, especially concerning the transparency of new customers while collecting the information and processing the data. Providing inadequate information of sources of money makes it harder to observe risks and signs of illicit financial actions which can also harm the customers. By following the KYC principle, the bank does not lose its obligation to process data confidentially. Institutions are required to follow corporate policies, legislation and are often monitored by Financial Authorities.[40]

3. General Data Protection Regulation

In chapter three, the study discusses the theoretical part of the GDPR, how the new Data Protection Regulation is affecting the European Union Member States. The chapter introduces the GDPR, analyses its relation to the previous version of the GDPR, what can be considered as a legitimate interest or legal obligation to process the data and the aim of balancing the interest. The study further continues to examine the relationship between the Charter of Fundamental Rights of the European Union in relation to the GDPR, and the problem areas concerning the GDPR.

[37] Ibid 169.
[38] Mark Nance, 'The regime that FATF built: an introduction to the Financial Action Task Force' (2019) Crime, Law and Social Change 1-21 123.
[39] Renny See Benedictus, Miru Ahmadi, Hasbir Muhadar, Paserangi, 'Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes' (2019) JL Pol'y & Globalization, 81-101 103.
[40] Ibid 104.

3.1 Introduction to the GDPR

In 2012, the Presidency of Council adopted the proposal of the General Data Protection Regulation (GDPR)[41] with a meaning to replace the old Directive 95/46/EC (The Data Protection Directive) [42].[43] The reason behind the proposal was to enhance the data protection rights of the individuals and improve the business world's data protection in the single digital market.[44] The Council proposed that the GDPR affect organisations outside of the EU who are transferring, goods, services or personal data through the EU.[45]

General Data Protection Regulation came into force twentieth day after its publication on the Official Journal of European Union, and it shall apply from 25 May 2018. It applies to all EU Member States and companies who are processing data through the EU.[46] The GDPR is the newest and one of the biggest steps taken in international data protection legislation. The GDPR gives more authority for private persons to influence the data collected about them, which means changes in data processing. The data process must be recorded, and individuals have the right to be aware of what kind of data is collected about them.[47]

The GDPR aims to protect individuals' data by making the data process being a responsible treatment of the data and making companies record the process of how the data is collected. The standards of processing data are set to high in the Regulation, and companies must have a legal basis to justify the data process.[48] The GDPR has brought more legal certainty to the data processing area by justifying the Member States legal framework and by introducing the legal grounds for processing data. Currently, almost every company is present in the digital sphere and are using digital services; processing data has become a key role in international corporations.[49]

Although the GDPR ensures individuals right to data protection, the right to protection of data is not an absolute right. It shall be considered in relation to fundamental rights and its function to society, together with the principle of proportionately,[50] also known as the principle of

[41] 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 (Data Protection Directive) [2016] OJ L119/1.
[42] 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.
[43] 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 (Data Protection Directive) [2016] OJ L119/1 article 94.
[44] Presidency of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach' (2012) Council of the European Union, COM/2012/011.
[45] 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 (Data Protection Directive) [2016] OJ L119/1 article 3.
[46] Ibid article 99.
[47] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 2.
[48] Ibid 2.
[49] Jan Philipp Albrecht, 'How the GDPR will change the world' (2016) Eur. Data Prot. L. Rev. 2 288.
[50] The Treaty on European Union [2016] OJ C202/01 (TEU) article 5.

fairness and justice.[51] Since the world is changing and technology is taking big steps in technological developing, processing data has changed, and the amount of the processed data has grown. Data processing has received more affect both in society and in the business world. Hence, it was necessary to do changes with the international framework concerning data processing. For preventing crimes, it is important to examine the interest between financial institutions collecting data and the right to protection.[52]

3.2 The GDPR replaces the Data Protection Directive

Since the Data Protection Directive failed in its aim, the EU decided to replace the Directive by starting to draft the GDPR in 2012 and introduced it in 2016.[53] In 2018, the GDPR had to adopted in all Member States. The negotiations and the process around the GDPR took four years to finalise the adaption of the Regulation. One of the most important differences between the GDPR and the Data Protection Directive is that GDPR as regulation has to apply directly to the national legislation without any implementation measures. The GDPR harmonises international legislation regarding data processing and towards greater legal certainty.[54]

The Data Protection Directive was adopted in 1995 in the EU on 24th of October. The Data Protection Directive aimed to protect individuals' data while processing and moving it. It ensured the fundamental rights of individuals regarding data processing. Since the Data Protection Directive was a directive and not a regulation, it was not directly applied to all Member States; in any case, the Data Protection Directive had to be transposed to the national legislation. Unfortunately, the Data Protection Directive did not fulfil its aim and did not live up to its objection. Legal issues arose concerning the implementation of the Data Protection Directive by the Member States. Since the Member States implemented and applied the Data Protection Directive indirectly to their national legislation, which arose issue that one data processing activity was allowed in another Member State, but in the other it was unlawful.[55]

3.3 Relationship between the Charter and the GDPR

The latest version of the Charter of Fundamental Rights of the European Union (The Charter)[56] came into force in 2016. The Charter aims to set out fundamental rights on the EU's area and protect them in the Charter. The Charter divided the fundamental rights under subtitles *dignity, freedoms, equality, solidarity, justice and general provisions*. These rights include right to private and family life and the right to protection of personal data under articles 7 and 8. Since the rights under the Charter are fundamental rights, it means that every Member State has to adopt the legislation to their national laws, are bound by it and the Member States national laws cannot limit it.[57] While processing the data, the GDPR cannot override fundamental rights and

[51] 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 (Data Protection Directive) [2016] OJ L119/1 recital (4).
[52] Tamara Dinev, 'Why would we care about privacy?' (2014) 23(2) European Journal of Information Systems <https://doi.org/10.1057/ejis.2014.1> accessed on 30 March 2019 97.
[53] 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 (Data Protection Directive) [2016] OJ L119/1 article 94.
[54] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 2.
[55] Ibid 2.
[56] The Charter of Fundamental Rights of the European Union [2016] OJ C202/02 (The Charter).
[57] Ibid article 52 (6).

freedoms; therefore, it has to be in accordance with the Charter, which is pointed out in the first recital of the GDPR as:

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.[58]

As mentioned in the previous paragraph, article 8 of the Charter plays an important role considering data protection and is considered as a legal framework for data protection. Article 8 of the Charter guarantees that everyone has the right of protection concerning their data, the data should be processed fairly for special purposes, there should be a legitimate basis for processing the data, individuals shall have the right to access the data collected about them, and the control is responsible that the mentioned rights are followed.[59]

As previously mentioned, article 7 of the Charter guarantees the right of respect for private and family life. Article 7 covers communication, which has to be in respect with the right to private life and family life, but the problem area was; what is considered as communication. Often the choice was left for a controller to decide. For instance, if an individual is updating open platforms, this cannot be considered as a confidential communication. Thus, it would not be safeguard by article 7 of the Charter.[60] Furthermore, the private and family life is continued under article 8 of the Charter, regarding data protection. Article 8 of the article can only be limited, as mentioned under article 8 (2) if there is a legitimate basis, and it is necessary to process the data which is similar to article 6 of the GDPR.[61]

For the financial sector, the problem was how to adopt article 7 in conjunction with article 8, concerning the definition of private life. Since the rights under the Charter are considered as fundamental rights, every sector, including the financial sector, has to be in agreement to rights under the Charter in the EU. The financial sector has established that the private area is often considered as home, not a business place. Article 7 of the Charter aims to protect the information which is wanted to keep as confidential information concluding *inter alia* people an individual is meeting. Based on this, it would be possible to assume that financial institutions do not fall under the scope of the article. However, article 7 and 8 are often considered together based on their similarity, which narrows article 7's scope on the special circumstances. For instance, business calls can be seen to fall under the aim of the article. Hence, for the financial sector, there has not been clear guidance of the scope of article 7 in conjunction with article 8 of the Charter.[62]

---

[58] 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 (Data Protection Directive) [2016] OJ L119/1 recital (1).
[59] The Charter of Fundamental Rights of the European Union [2016] OJ C202/02 (The Charter) article 8.
[60] European Data Protection Supervisor, 'Formal comments of the EDPS on a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market' (2018) The EDPS 5.
[61] European Union Agency for Fundamental Rights, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union – Volume II – Summary' (2018) European Union Agency for Fundamental Rights 1.
[62] European Union Agency for Fundamental Rights 'Handbook: Preventing unlawful profiling today and in the future - a guide' (2018) European Union Agency for Fundamental Rights 31-33.

3.4 Right to Erasure and Right to Data Portability

3.4.1 Right to Erasure

The GDRP introduced article 17 of the GDPR "Right to erasure" or more familiarly "right to be forgotten" which gives individuals the right to request the erasure of the information collected about them. If there is not a legitimate reason to deny the request, authorities are obligated to delete the data. Article 17 of the GDPR was one of the major changes in data processing and limited firms right to save and collect information. Because of the GDPR, authorities are obligated to give the information collected from individual and remove it if the individual so requests. After the GDRP authorities are allowed to collect only the necessary information for the use of the data.[63]

The right to be forgotten was discussed on the Court of Justice of the European Union (CJEU) in case of *Google Spain*[64] in 2014. In the case, a Spanish citizen Mario Costeja González requested his name to be removed from a webpage, which collected information of people who have been forced to sell their property based on social security debts. He requested the removal of the information since the article was no longer relevant, and the article appeared on the Google search engine while searching his name. Webpage, the owner of the article, refused to remove the information. Therefore, Mario Costeja González contacted the Spanish Data Protection Agency, which led to receiving a refusal from Google Inc., who received the task from Google Spain. Since Google Inc. is located in California, they argued that it did not fall under the scope of the old Data Protection Directive, and Google Spain is not responsible for Google's search engine.[65] Google continued to argue that the information regarding the webpage and article does not fall under the description of personal data and Google cannot be regarded as a data controller.[66]

The case was taken into CJEU in 2013, and the judgement was given in 2014. The court ruled that the search engine operator, in this case, Google Inc., is responsible for the data presented in webpages that appear on the search engine. The court also concluded that Google Inc. falls under the territorial scope of the Data Protection Directive since Google Inc. is part of Google Spain, and besides falls under the scope of "Data Controller" according to article 2 (b) of the Data Protection Directive. The court balanced the interest between Mario Costeja González (data subject) and Google (the data controller) with the help of the Charter of Fundamental Rights of the European Union (The Charter).[67] The court took into account with article 7 right to private life and article 8 protection of personal data of the Charter. The previous version of article 17 of the GDPR, article 12 (b) of the Data Protection Directive rules that the data subjective can ask an erasure of his or her personal data.[68] The controller shall examine the request and agreed if there are no legitimate grounds to refuse to erase the data. The court concluded that considering the right to be forgotten, unnecessary and irrelevant information

[63] 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 (Data Protection Directive) [2016] OJ L119/1 article 17.
[64] 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.
[65] Ibid para 21, 42.
[66] Ibid para 62.
[67] The Charter of Fundamental Rights of the European Union [2016] OJ C202/02 (The Charter).
[68] 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 para. 97-99.

might be incompatible with the Data Protection Directive, in such case the data shall be erased.[69]

3.4.2 Right to Data Portability

In article 20 of the GDPR, the Regulation introduced the right to data portability. Article 20 of the GDPR states that the data subject, a person whose data has been pursued to a controller, or in a register, has right to receive the personal data collected about the individual and right to transmit the data to another controller or another register without any hinders.[70] Article 20 of the GDPR applies if the data process is automatized, mentioned in article 20 (2), or the data subject has given his or her permission to process the data. Thus, there must be a mutual agreement to process the data, mentioned in article 20 (1), which also has to be included when transferring the data to another controller. However, article 20 has exceptions considering processing data. It cannot restrict applying article 17 of the GDPR and article 20 shall not be applied when processing necessary information in the light of public interest. Article 20 of the GDPR can be limited if there is a legal obligation or legitimate interest to process or if a contract has limited the article 20.[71]

3.5 Legal Obligation and Legitimate Interest

Article 6 of the GDPR discusses the lawfulness of the processing. Regarding article 6 of the GDPR processing data shall be lawful when it is necessary on the grounds that there is a legal obligation or legitimate interest to process the data. Article 6 (1) (c) of the regulation rules following: "processing is necessary for compliance with a legal obligation to which the controller is subject"[72] and continues in article 6 (1) (f) of the GDPR:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[73]

As mentioned in the previous paragraph, right to process cannot be limited if there is a legitimate interest to process the data if interests of fundamental rights and freedoms do not override the interest, for instance, if the data subject is a child, the data subject requires protection of his or her data.[74] The wording of the previous article is ambiguous, but as the article implies, the data process shall be lawful, if the result of balancing the interest, the legitimate interest of the controller or, a third-party, is more necessary than protecting the data.[75]

---

[69] 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 article 6 (1) (e), 6 (1) (f).
[70] 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 (Data Protection Directive) [2016] OJ L119/1 article 20.
[71] Ibid article 20 (4).
[72] Ibid article 6 (1) (c).
[73] Ibid article 6 (1) (f).
[74] Ibid article 6 (1) (f).
[75] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 103.

Legal obligation means that the person processing the information, *inter alia* controllers, have a legal duty and particular reason to process the individual data, it can be permitted. In other words, the process shall be legal if it is following legal obligations. However, as mentioned in recital 45 of the GDPR, if there is a legal obligation to process the data, the legal grounds must be laying in the EU or Member State law.[76] An example of this kind of scenario is national tax legislation, which can cause a necessary reason to process data even if the individual does not agree.[77] Article 6 (1) (c) is in a key role to correspond for former legal permissions under the Data Protection Directive. Article 6 (2) presents that the Member States are allowed to introduce more specific provisions to adapt the application for determining legal permissions for special requirements regarding article 6 (1) (c) and (e).[78]

Article 6 (1) (f) introduces a general cause, which can give a legitimate interest to process the data without mutual agreement. The article means that processing the data without mutual agreement is lawful if it is necessary for the purpose of legitimate interest. In case the legitimate interest is applied, the controller has a burden of proof which can be *inter alia* economic and financial interest, and is necessary to process.[79] Legitimate interest applies if the interest has a legitimate ground; it is important to recognise that the limitations in relation to protecting personal data are applied when it is absolutely necessary. For instance, in the CJEU's case, *C-13/16*[80] ruled that in some cases, it is necessary to receive *inter alia* address and identification number if first name and surname are not enough. In the present case, the Court ruled that the personal data was necessary to receive personal information of the person who damaged their property to sue the person. The Court ruled that the present case fills the legitimate interest's criteria.[81] The GDPR recognises, *e.g.* preventing fraud as a legitimate interest or ensuring network and information security. IT-systems saving data that can be connected to a fraud or a criminal action have to be committed to the security services, an example of this kind of action would be illegal use of the network by an unauthorised author.[82]

3.5.1 Balancing the Interest

The balancing of interest can be problematic. In CJEU's case, C-13/16 the Court rules that balancing the legitimate interest is circumstantial and depends on the individual case.[83] Balancing the interest includes a careful implementation of specific processing situation. When analysing the balance of interest, three aspects have to be concerned.[84] Firstly, the legitimate

[76] 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 (Data Protection Directive) [2016] OJ L119/1 recital (45).
[77] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 108.
[78] 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 (Data Protection Directive) [2016] OJ L119/1 article 6 (1).
[79] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 103.
[80] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'* [2017] OJ C213/11.
[81] Ibid para. 29-30.
[82] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 104.
[83] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'* [2017] OJ C213/11 para 31.
[84] 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 (Data Protection Directive) [2016] OJ L119/1 recital (49).

interest of the controller or third-party have to be balanced out, secondly the necessity of the processing in the light of these legitimate interests and thirdly, there cannot be overriding interests or rights of data subjects.[85] While analysing the data process and the legal base of it, individuals' rights must also be considered during every specific processing situation.[86] If the ground for legal basis is found after examining the balance of the interest, the data process cannot be prohibited. In CJEU's case, C-13/16, the Court noted that legitimate interest could not be applied to personal data of racial origin or political opinion. However, address, name and id number can be requested and given after balancing the interest of an individual case.[87]

3.6 Problem areas considering Financial Crime Data Process under the GDPR

The GDPR necessitates legitimate grounds or an agreement to process the data. If a person has given his or her permission to process the data on special purposes, the purpose of processing data is connected to the legal obligation or legal interest, or processing data is necessary for the performance of a contract the data processing shall be legal.[88] The GDPR emphasises the necessity of the task to perform it. Due to this, the GDPR does not apply smoothly to every legal area. In the financial industry, the whole context of the GDPR changed the way of how to process data. The GDPR sets high requirements for processing the data and to the consent of data. While processing data, the company must have permission to use it, in addition the company has to hold a record of how the data is processed and used.[89]

The next problem on the financial industry is the GDPR giving the right to customers to withdraw whenever they want or even ask to erase their data under article 17 of the GDPR. As long as there is not a compelling reason to save the data, individuals have the right to be "forgotten" and withdraw their data. Right to be forgotten affects financial institutions, which are usually accustomed to dealing with large amounts of data. The ruling under 17 also affects to third-party organisations who are sharing the data with financial institutions.[90] Article 17 of the GDPR sets higher standards for data processing, and financial institutions are obligated to find justification for processing the data. This means that financial institutions have to limit the amount of data they are processing, which affects *inter alia* collecting information under the KYC principle.[91]

One of the most affecting changes after the GDPR was the consequences of a breach. If the GDPR is breached, for instance by security leaks or unauthorised individual being able to access the data, the institution has, according to the article 33 of the Regulation, 72 hours to inform the supervisor authority after the breach was detected. Under article 33 (4) the GDPR allows a longer timeline to provide the information in phases if the full investigation cannot be done in 72 hours.[92] Breach of the GDPR can cause a 20 000 000 EUR or four per cent of global revenue

[85] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 105.
[86] Ibid 106.
[87] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'* [2017] OJ C213/11 para 29.
[88] 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 (Data Protection Directive) [2016] OJ L119/1 article 6 (1) (c) and (f).
[89] Ibid article 6.
[90] Ibid article 17.
[91] Malish, Richard, 'Financial Crime and Compliance under GDPR' (2018) NICE Actimize 1-11 7.
[92] 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 (Data Protection Directive) [2016] OJ L119/1 article 33.

fine for the company. In case of a breach, the safety measures the company took will be determined by regulators. The regulators will analyse the accountability of the company, which means that companies have to show their compliance in accordance with data protection on how their data controllers are functioning.[93]

Lastly, the GDPR has received some criticism concerning the harmonisation between the Member States. Since the GDPR has many provisions referring to the Member States legislation and that the GDPR reminds more of a directive than regulation. Though, considering the difference between a directive and a regulation affects to the implementation of legislation since the GDPR leaves only exceptional and limited powers to the Member States which can only be applied and justified with legal obligations.[94] By comparing the Data Protection Directive and the GDPR, the difference between the Directive and the Regulation is significant. The Data Protection Directive did not fulfil its aim to harmonise the legal framework considering the data protection of citizens of the Member States of the EU nor on the financial sector. The GDPR sets higher standards and is stricter on processing data. What comes to children and sensitive categorised data, the rights of an individual are emphasised under the GDPR. While processing personal data of children or sensitive categorised data, the controller has stricter rights to the process, and the data cannot be justified under the legitimate interest similarly than personal data of other groups. Since the GDPR is a regulation, the Member States had to interpret the regulation in the national law without changes or states' interpretation. On the financial sector, this means justify the processed data with legitimate grounds and limit the amount of processed data. The financial sector has to record the process of data collecting and prepare themselves on withdrawal of data under article 17 of the GDPR or being able to extradite the data for a data subject when it is requested under article 20 of the GDPR.

4. 5th Anti-Money Laundering Directive

In the fourth chapter, the 5th AML is introduced. The chapter discussed money laundering and financial crime data under the 5th AML; in addition, the chapter presents the Anti-Money Laundering Directive saga and history behind the directives. The chapter examines the relationship between the 4th AML and the 5th AML and continues to examine the Directive ruling about data processing, especially regard to financial crime data and KYC principle.

4.1 Relationship between earlier Anti-Money Laundering Directives and the 5th Anti-Money Laundering Directive

The 5th AML is the fifth version of the series of Anti-Money Laundering Directives. The First Anti-Money Laundering Directive[95] was adopted to the EU law in 1991 to protect the Union from financial crimes. The first Anti-Money Laundering Directive includes 18 articles and gave obligations to customer knowledge under the financial industry. The first directive also emphasises the relationship between the Member States and harmonises the legislation, but since it was the first version of Anti-Money Laundering Directives, it only gave short guidance and ruling on the directive's area.[96] The first directive was later used as a base for the second and third Anti-Money Laundering Directives, and it helped to recognise the problem area.

[93] Ibid article 83.
[94] Jan Philipp Albrecht, 'How the GDPR will change the world' (2016) Eur. Data Prot. L. Rev. 2 287.
[95] Council Directive (EC) 91/308 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/77.
[96] Ibid preamble.

The Second Anti-Money Laundering Directive[97] was established in 2001, ten years after the first one. The second directive included five articles of amendments for the first directive and aimed to update the ten-year-old version of the directive. The second directive fulfilled the gaps pointed out in the 40 recommendations of annual (1996) report of the FATF considering the wider definition of money laundering.[98] The first directive did not apply adequately to the Member States' authorities considering changing details for customer information and suspicious acts.[99] The second directive applied a broader definition of criminal activity, including corruption and broader application for predicate crimes. The second directive also implied that lawyers have right to participate in financial transactions.[100]

The Third Anti-Money Laundering Directive[101] replaced the second directive in 2005, after four years of the second directive introduced its amendments to the first one. The third directive concentrated especially on FATF's recommendations and extended a wider definition of financial crimes. The preamble of the third directive indicates that even crimes, which are usually not analysed as financial crimes, should be noted in preventing financial crimes. The third directive gave more attention to legal professionals in the scope; in fact, the directive notes all professionals working in the financial industry. To give a wider application to other professions is a huge change from the earlier directives. The third directive also emphasised measures for the politically exposed individuals in accordance to customer due diligence and emphasised transparency in all levels to prevent corruption.[102] These were the biggest changes compared to the two previous directives.[103]

4.2 Introduction to the 5th Anti-Money Laundering Directive

The European Union introduced 5th Anti-Money Laundering Directive (5th AML)[104] on 30th of May 2018. Like the second Anti-Money Laundering Directive, the 5th AML includes only six articles and concentrates on amending the 4th AML. The 4th AML and the 5th AML are functioning closely together; the 5th AML is replacing and adding information to specific provisions under the 4th AML and updating the legal framework of the directives. The 5th AML points out in its recitals the relationship and importance between the 5th and the 4th AML. The recitals of the 5th AML points out the 4th AML shall be considered as the most important framework preventing financial crimes and money laundering.[105] Since 5th AML is a directive, it gives the Member States right to adopt it fully to their national legislation, but as a directive, the 5th AML also leaves room for implementation to the Member States national legislation. The 5th AML presented a new type of ruling on customer due diligence and put pressure on financial institutions to know their customers and prevent risks concerning business partners.

[97] 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.
[98] Ibid recital (7).
[99] Ibid recitals (3) (13).
[100] Ibid article 2.
[101] 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.
[102] Ibid recitals (20) (25).
[103] Ibid recital (25).
[104] 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.
[105] Ibid recital (1).

Last terrorist attacks in Europe have affected and changed crimes in the financial sector, which was noted on the 5th AML. The 5th AML aims to co-operate with financial institutions by updating legislative to be in account with current issues. The 5th AML concentrates on adding amendments to virtual currency and Fiat currencies, but this shall not be mixed with electronic money, which is defined on article 2 of Directive 2009/110/EC of the European Parliament of the Council[106] and covered in Directive 2015/2366 of the European Parliament and the Council[107].[108]

Furthermore, the 5th AML targets to lower the use of anonymous transactions, and aims that payments of over €50 cannot be carried out in online, or over €150 payments on stores with prepaid credit cards.[109] Lastly, the 5th AML sets standards to co-operate with high-risk third countries, meaning countries that are not the EU Member States and have not applied necessary elements to tackle issues with corruption and money laundering. While accessing a business relationship with the high-risk third country, the 5th AML demands to act carefully and secure.[110]

It is important that the financial sector, institutions and authorities are together working against financial crimes by applying and strengthening measures against the crimes. Since this is a global issue, the EU co-operating with different organisations to receive advising from business-related industry to create legal framework. In the 5th AML, the EU applied the FATF recommendations together with Egmont Principles to ensure ruling regarding preventing and fighting against money laundering in the directive to reach international recognition. The directive suggests that preventing money laundering is something which has to be considered at international, national and working level.

4.3 Relationship between the 4th and 5th Anti-Money Laundering Directives

The 4th Anti-Money Directive (4th AML) was adopted on 20th of May 2015 and interpreted to Member States' national legislation on 26th of June 2017.[111] After ten years of using the third directive, it was time to update the legal framework in regard to financial crimes, which led to the Fourth Anti-Money Laundering Directive. The 4th AML aims to prevent flows of illicit money, strengthening the risk assessment obligation on the financial sector, prevent money laundering and prevent terrorism financing.[112] The Directive continued to emphasise customer knowledge from the third one and introduced a new term *holistic risk-based approach*, which means evidence-based decision-making while analysing high risks and risk status. The 4th

[106] Council Directive (EC) 2009/110 of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7.
[107] Council Directive (EC) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35.
[108] 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 recital (10).
[109] Ibid article 1 (15) (g).
[110] Ibid article 1 (11).
[111] 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 article 69.
[112] Ibid recitals (1)-(4).

AML is often described as the biggest and most effective anti-money laundering directive with its wide application and strengthen ruling considering financial crimes.

The 4th AML was used as a ground for the 5th AML, and the Directives are co-operating with the 4th AML 69, in addition, six articles of the 5th AML. Both Directives are into force at the moment, but the 5th AML is the current one. The 5th Directive made necessary changes to the 4th AML, for instance concerning data protection legislation by replacing the Data Protection Directive under the 4th AML to the GDPR.[113] Another change the 5th AML takes compared to the 4th AML is central beneficial ownership register. The 5th AML pursues that the central beneficial ownership register would be more open for the Member States and the Member States should use European Central Platform for exchange the data.[114] This would mean to have more public databases for the Members of the EU.

4.3.1 The future of next Anti-Money Laundering Directive

The sixth Anti-Money Laundering Directive is published, and the transposition date is set on 3rd December 2020.[115] The sixth directive, including 16 articles, follows the saga of Anti-Money Laundering Directives and strength *inter alia* the criminal aspect of Anti-Money Laundering Directives. The sixth directive introduces a maximum term of imprisonment of at least four years.[116] The other notable change in the sixth directive is that environmental crimes are falling within the scope of the directive.[117] The sixth directive is similar to the 4th AML and 5th AML and completes them on criminal liability. While the 5th AML concentrated on e-currency and transparency, the sixth directive will concentrate more on criminal nature and punishment on money laundering and harmonising it between the Member States.[118]

The sixth directive will continue to put accountability for companies. As the earlier directives, the sixth directive will also focus on preventing money laundering and gives obligations to the companies to follow. According to the sixth directive, legal persons can be held liable for the crime based on lack of supervision, which means that *e.g.* head of the company can be found guilty of lack of control.[119] All Member States shall imply the laws under the sixth directive to their national legislation and comply with the national legislation by 3 December 2020.[120]

4.4 Processing Data under the 5th AML

In the preamble on paragraph five of the 5th AML, the directive states that collecting personal data should be concerned together with fundamental rights and fundamental rights should be fully respected in the process, as well the principle of proportionality. Institutions are only allowed to process the data the way the directive rules.[121] The legislation introduced ruling on

[113] 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 article 1 (26). [Previously article 43 of the 4th AML].
[114] Ibid article 1 (15) (g).
[115] Council Directive (EC) 2018/1673 on combating money laundering by criminal law [2018] OJ L284/22 article 13.
[116] Ibid recital (14).
[117] Ibid recital 2 (1) (5).
[118] Ibid recital (5).
[119] Ibid article 7 (2).
[120] Ibid article 13.
[121] 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 recital (5).

processing data in the 4th and 5th AML directive, which is something that previous anti-money laundering directives did not have. The 5th AML, together with the 4th AML, concentrated more on how to lawfully process the data while still preventing money laundering legally. Protecting individuals' private life is a fundamental right, protected by The Charter article 7, 8 and 16; the ECHR article 8; and TFEU article 16, also protected by the GDPR. Thus, the 5th AML cannot override fundamental rights and freedoms, which the Commission has noted on their rapport on the implementation of the Directive.[122] In addition, the 5th AML is presenting requirements that organisations have to follow and ensure. According to article 1 (26) of the 5th AML, processing data under the article should be considered together and read in light of public interest and the GDPR, which replaced the Data Protection Directive. Aim of article 1 (26), earlier article 43 of the 4th AML, is to harmonise the use of data and data protection in the Member States.

> The processing of personal data based on this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Regulation (EU) 2016/679 of the European Parliament and the Council (*).[123]

The GDPR affects a large area; thus, it affected even the 5th AML directive. Earlier, the Anti-Money Laundering directives followed the Data Protection Directive, but the changes were noted on the 5th AML added an amendment considering the Regulation. The European Data Protection Supervisor (EDPS) gave propositions and their opinion[124] to develop data protection under the 4th AML and was consulted while constructing the 5th AML, especially with article 28 (2).[125] The opinion is directed for the Council as a proposal while drafting a new legislation.

The EDPS is a supervisor authority who ensures that European Union institutions are following data protection laws and respecting the right to data protection. The EDPS has three main fields they are working on; firstly, supervision when they are monitoring that the EU is following the data protection rules; secondly, consultation when the EDPS is advising the European Commission, the European Parliament and the Council on proposal for a new legislation and; thirdly, cooperation between the EDPS and the Member States national data protection authorities (DPAs) to help promote data protection rules across the EU.[126]

The EDPS presents the principle of purpose limitation, which proposes that the Anti-Money Laundering Directive shall process and collect personal data for special purposes. The directives aim to prevent money laundering and the proposal mentions fighting against financial criminality. However, the EDPS presents its considerations in the proposal about the amount of processed data. In the proposal, the EDPS points out unclarity on the Anti-Money Laundering

[122] Ibid recital (51)-(52).
[123] Ibid article 1 (26).
[124] The European Data Protection Supervisor, 'EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC: Access to beneficial ownership information and data protection implications' (2017) The EDPS.
[125] 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 recital (54).
[126] The European Data Protection Supervisor, 'Annual Report 2018' (2018) Publications Office of the European Union 9.

Directives considering data processing and how the data processing rules are affecting the information collected under Anti-Money Laundering Directives.[127]

The 5th AML requires in article 2 (25), earlier article 40 of the 4th AML, that financial institutions shall retain the data and information for purposes of preventing, detecting and investigating possible money laundering and other financial crimes. However, the data related to business relationship shall be removed after five years of customer relationship have ended or after the date of an occasional transaction.[128]

4.4.1 Financial Crime Data under the 5th AML

Collecting of financial crime data plays an important role considering of preventing illicit financial flows. If the financial crime data is not collected early enough, it will make it harder to prevent money laundering and financing terrorism, or in the worst scenario, it will not be noted at all. Therefore, it is important to develop a register which collects necessary information. That would mean the information would be available quickly for all the Member States.[129] The financial crime data would include a data of a person who has committed a financial crime, has been connected to financial crime or there is a suspicion of criminal activities, connected to *inter alia* money laundering.[130]

Under the 5th AML financial crime data involves both legal and natural persons. Persons dealing with large amounts of money are obligated to apply to anti-money laundering safeguards which are listed in the 5th AML article 1 (previously the 4th AML article 2 [1]). The list includes *inter alia* lawyers, tax revisors and external accountants but even the personal data scope is very wide in the 5th AML.[131] If the financial authority finds suspicion information while processing data, they are obligated to inform Financial Intelligence Unit (FIU) which task is to carry out the information to the Member States and cooperate between the Member States.[132]

---

[127] The European Data Protection Supervisor, 'EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC: Access to beneficial ownership information and data protection implications' (2017) The EDPS paragraph 13.

[128] 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 article 2 (25).

[129] Ibid recital (20).

[130] 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://doi-org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 28th April 2019 116.

[131] Ibid 118.

[132] 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 article 1 (21). Previously 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 article 33.

4.4.2 Know Your Customer under the 5th AML

The 5th AML aims to harmonise the KYC rules in the Member States. The 4th AML introduces KYC principles in its second chapter, which it amended in the 5th AML.[133] The directive obligates to have an identity of a customer before entering into a business relationship, meaning that if the customer is not providing legitimate identification, he or she shall be excluded from all business-related action. Also, financial transactions carried out by banks must be examined before processing it through to prevent money laundering.[134]

The 5th AML introduces legislation that the customer data for money laundering investigations should be saved on automatically functioning register or data retrieval systems in financial institutions which would help to process the amount of data. The Member States should be allowed to have an impact to determine which information they shall collect to have a full understanding of beneficial owners of companies.[135]

The reason behind KYC rules is to learn to know the risk basis behind the business relationship and analyse the connection between the money laundering and financing terrorism. Unfortunately, risk-based customer analyses are not always noticing a certain type of risks. Therefore it is important to have a risk-based analysis of customers and specified categories for already existed customers, which can be monitored.[136] The 5th AML supports to have a more open database for customer information and to have public access to it so that the Member States can share data. To have public access to beneficial ownership would strengthen society's possibilities to receive better information about the customer relationship and beneficial owners, *inter alia* journalists and organisations could contribute to share the information.[137] Since of the GDPR came into force and it co-operates with the 5th AML financial institutions have to find a way to process the data through the complexity of the legal system without losing the aim of the KYC principle.[138]

5. Analysis of Processing Financial Crime Data under the GDPR in the light of the 5th Anti-Money Laundering Directive

In this chapter, the study analyses the findings of the study regarding the GDPR in light of the 5th AML. In this chapter, the study compares the Regulation, and the Directive regarding the data processing in light of financial crime data. The study also analyses the changes after the GDPR came into force and the impact the Regulation has. The analysis is based on the material presented in the previous chapters by examining the theoretical parts of the study.

---

[133] 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 chapter II.

[134] 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://doi-org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 28th April 2019 118.

[135] 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 recital (21).

[136] Ibid recital (24).

[137] Ibid recital (30).

[138] Laura Glynn, 'KYC vs Data Protection – The next compliance hurdle' (2016) Fenergo 12.

5.1 Introduction

Data processing and financial crimes are current legal issues which have been put more and more on focus on nationally and internationally. Legal framework on both areas has been developed through the years, and processing financial crime data has become an important legal issue. Nowadays, financial crime data has been taken into more concertation, it is applied wider, and the legal framework has become stricter to prevent inadequate use of personal data and prevent to receive benefit from illegal financial flows. The financial sector has an important role in monitoring transactions, banking, and preventing money laundering. To receive all the necessary information for monitoring, the financial institutions have to process large amounts of data through the organisation. Therefore, financial institutions have a strong connection to personal data and GDPR.

The GDPR and data processing have an important relationship to money laundering. In the financial sector, one of the biggest challenges is to manage the amount of data processing and KYC principles. After the theoretical part of the study, the study has found out that personal data plays an important role in the digitalised financial sector. Since of the GDPR, the process of collecting personal data is stricter, and individuals have more ways to affect the data collected about them. Previously, the Member States could adopt the Data Protection Directive's aims to fit the national law, but the GDPR as a Regulation became immediately applicable and enforceable without interpretation to all Member States.

Types of financial crimes have changed during the years, and the latest events had affected the way how to structure and draft a directive and regulation. The legal framework has been updated after the recent events took place in the world — for instance, terrorist attacks in Nizza, the 9/11 in the USA and Madrid. One of the major changes affecting the money laundering and financial crimes is data processing, and the way the internet has changed it. Financial crimes have become more common and taking benefit of different internet servers and services. Therefore, the legislation has to keep up with the development.

5.2 Changes after the GDPR

After the GDPR came into force, individuals received more rights considering their data and more strict rules for the companies. By strengthening the ruling considering the data means that the financial industry had to go through some changes to fully follow the ruling under the Regulation and applied the GDPR fully to their process. The GDPR is largest change happened on data processing and harmonising the way to process the data in the Member States, the aim behind the Regulation is to protect individuals' rights in the digitalised world.[139]

The protection of personal data was already discussed on the Data Protection Directive; however, it was not foreseeable how the data processing is going to develop through the years. The growing amount of data has caused an issue concerning how much privacy there shall be and where is the line between necessary and unnecessary data processing. The GDPR is described as one of the most powerful data protection legislation. The GDPR ensured individuals rights under right to be forgotten and right to access the collected data, the penalty of the data breaches was set to higher, and the GDPR strengthen the ruling concerning the

[139] 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 (Data Protection Directive) [2016] OJ L119/1 recital (6).

legitimate obligation and legal obligation which the Member States had to adopt directly to their national laws.[140]

Since the financial industry is processing a lot of data daily, it is obvious that the GDPR changes the way they are able to process it. After the changes of the GDPR financial institutions have to have a legitimate interest or legitimate obligation to save the information, this means that the financial industry must have a mutual agreement between them and person whose data is processed or there has to be a legitimate obligation or interest to process it. [141]

5.3 Analysis of Data Processing under the GDPR in the light of the 5th AML

The need for regulation for data has arisen since the amount of data processing has growth. The problem has been to find a strict way to process the data and harmonise the Member States way to adopt the legislation. The data processing rules under the GDPR are considering individuals rights to affect the data collected about them, and it sets high standards, for instance, for financial institutions to process the data. Previously, the problem was the Member States own interpretations of the Data Protection Directive and the lack of updated legislation concerning the newest research of data protection.

The protection of personal data was not only covered in the replaced Data Protection Directive but *inter alia* in the Charter. The Charter includes fundamental rights and freedoms of the European Union, and is still in force and included into the GDPR. However, the problem concerning data processing was the Charter's wide wording and the issue regarding how much privacy people shall have while processing their data. The Charter includes two articles relevant to data processing, right to private and family life and protection of personal data. Article 8, protection of personal data, has similar actors as article 6 of the GDPR, but article 8 includes more general ruling while article 6 of the GDPR gives stricter guidance of the lawfulness of the processing.[142]

The ruling under the GDPR differs from the 5th AML. As the GDPR gives clear guidance of lawfulness of processing, the 5th AML discusses data processing shortly in waves to the GDPR. Data processing under the 5th AML is concerned widely and mostly concentrates to databases for beneficial owners. The 5th AML suggests that the databases should be more open for public interest and to prevent financial crimes.[143] Contrary to the GDPR, which aims to protect individuals' data and minimise the amount the institutions are allowed to process. Although the 5th AML is a directive concentrating to preventing money laundering, based on the importance of processing data, the next Anti-Money Laundering Directive could include stricter and clearer ruling concerning processing data, for instance, the Directive could imply legal basis concerning the GDPR article 6's legal obligation and legitimate interest. This change would make clearer guidance for financial institutions creating an efficient way to process the data and include legal certainty to processing financial crime data between the Member States.

[140] Ibid article 6 (1).
[141] Ibid article 5 (1).
[142] European Union Agency for Fundamental Rights 'Handbook: Preventing unlawful profiling today and in the future - a guide' (2018) European Union Agency for Fundamental Rights 31-33.
[143] 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 recital (38).

5.4 Does the GDPR Complicate Processing of Financial Crime Data?

In general, the GDPR applies when there is an agreement to process the data. This has provoked a question concerning processing financial crime data to prevent financial crimes and if so, does the financial institutions need the consent of data subject. Often, customers are willing to give their permission to process the data for banking services in order to prevent money laundering. Individuals are still having the right to withdrawal their data and the right to access the data concerning them.[144]

Even the legitimate interest can be concerned as a legal basis for processing the data. However, legitimate interest shall be balanced to avoid overriding of the interest. For instance, if the legitimate interest is not in balance with fundamental rights, the legitimate interest can be limited. This creates a complexity between financial institutions and the legitimate interest, the wide application of term legitimate interest can be hard to apply in the financial sector.[145] Although legitimate interest includes a wide scope, the GDPR states that data which is necessary to process to prevent a fraud falls under the scope of the article. Many of the financial crimes fall under the description. Hence, the legitimate interest could be applicable while processing financial crime data.[146]

As for a finding of the study, the GDPR is permissive to process the data regarding preventing financial crimes. In most of the cases, the financial crime data can be processed under the legitimate interest or legal obligation, which is ensured in article 6 (1) of the GDPR. In addition, financial institutions have started to inform their customers that they have a legal obligation to process the data if there is a question of money laundering or included legal obligation as potential justification.[147] The 5th AML can support legitimate obligation and legitimate interest. The difference between the 5th AML and the GDPR is that the 5th AML aims to prevent financial crimes and aims directly to the financial crimes, whereas the GDPR concentrates only on the protection of individuals data.

However, having a clear description of a legitimate interest would help the financial sector to adopt it as a legal basis for processing the data. The issue concerning article 6 (1) (c) and 6 (1) (f) is to how to fulfil the aim of the articles. For instance, the EDPS or the FATF could give special opinion and recommendations concerning processing financial crime data under the GDPR in regard to the legitimate interest and legal obligation to process. The existing documents do not include enough clear guidance of the application of these articles. Financial institutions are going through a lot of changes considering their habit to collect the data.[148]

5.5 Analysis of Know Your Customer Principle under the 5th AML in regard to the Data Protection

As we have learned, personal data has a close connection to money laundering, especially regarding KYC principles. Both the 5th AML and the GDPR are comprehensive legal frameworks affecting on a national and international level. The data processing has increased

[144] See chapter 3.5.
[145] See chapter 3.5.1.
[146] 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 (Data Protection Directive) [2016] OJ L119/1 article 6 (1) (f).
[147] See chapter 4.4.1.
[148] See chapter 3.6 and 4.4.

lately, as it has money laundering, which has caused the need for protection of personal data. For the financial sector, it has been hard to keep up with new data protection rules and to be sure how to adopt the legislation considering the lawfulness of data processing and, for instance, KYC principles. For financial institutions, it is important not to lose the effectiveness of data processing while completing legislation.[149]

After the GDPR came into force, data controllers, have received stricter requirements considering the data processing. Without legal grounds, financial institutions have to assign the collected data considering the data subject. Processing the data in regard to legitimate interest causes problematic considering its ambiguous scope, which can be hard and risky to apply to the financial sector. Also, people are not aware of the importance of collecting personal data in relation to KYC principles. For the financial institutions, it is important to collect the necessary information of their customers to be able to accomplish risk-based analysis and investigate the risks the institution is taking.[150]

The reason behind the KYC principle is to learn to know the business partner before entering to business relationship to help to prevent money laundering and other financial crimes. The KYC also helps to prevent financial loses for the institutions and minimising the financial threat for both the institution and customers of the institution. In the EU, the KYC principle is ruled under the 5th AML. Financial institutions process large amounts of data on a daily basis, considering both private persons and legal persons. Previously, there has not been clear guidance considering financial institutions collecting the customer data and even now there are still some issues for financial authorities to adopt legislation regarding customer due diligence. It is not clear if the legitimate interest can be applied while processing the data. The data process shall be lawful if there is an agreement between the controller and the data subject, but unfortunately, not everyone is willing to give their permission to process the data for special purposes. Therefore, there is a need for jurisdiction concerning the data process in light of the KYC principle. For instance, the next Anti-Money Laundering Directive could include a special provision concerning the collection of information based on customer due diligence, or it could be included under the GDPR. It would lead to stronger legal certainty and harmonise the process between the Member States. The FATF has given recommendations considering the KYC principle which the EU could exploit while building up the next directive or regulation concerning KYC principles.[151]

5.6 Balancing the Interest of the Rights

The GDPR introduced under article 6 (1) (f) legitimate interest which allows processing the data without agreement as learned from the previous chapters; it has not been defined exactly how the legitimate interest can be applied. In the case of C-13/16, the Court ruled that the legitimate interest has to be balanced in every separate case, and the definition of it is circumstantial which making is balancing the interest problematical. By examining the interest, the controller's interest has to be analysed, the necessity of the process shall be analysed, and the interest cannot override the interest or rights of the data subject. If legitimate grounds find the legitimate interest, the data process shall be lawful without agreement between the data controller and the data subject.[152]

[149] See chapter 2.3.
[150] See chapter 4.4.2.
[151] See chapter 4.4.2 and chapter 2.3.
[152] See chapter 3.5.1.

Processing personal data is a fundamental right guaranteed by, for instance, under articles 7 and 8 of the Charter. Fundamental rights and freedoms are guaranteed for every citizen of the EU Member State and cannot be overridden. These rights are recognised in both the GDPR and the 5th AML in the recitals of the Regulation and the Directive. The Charter sets a minimum level of protection of personal data under articles 7 and 8, considering the right to private and family life and protection of personal data and the rights must be recognised and ensured by the Member States. Processing data is not an absolute right, yet article 8 of the Charter can be limited in the special circumstances, *inter alia* if there is a legal obligation to process the data.[153] However, while balancing the interest, the principle of proportionately shall be considered as well. The limitation of the fundamental right has to be concerned as fair and justified to achieve the balance.

The GDPR has helped to process of balancing the interest and in consideration of the principle of proportionately by strengthening the protection of personal data. Considering the balance of interest and balancing the fundamental rights, the financial sector has had a problem with adopting the rights in the data process. First of all, article 7 of the Charter includes private life and family life, which in general is considered as a home. Hence, financial institutions nor business places do not fall under the scope of article 7. Secondly, the wording of article 8 is widespread in financial crime data's view. The conflict between protecting personal data and money laundering rules are based on the challenging balancing of requirements between the two legal frameworks and balancing of the interest imposed of the financial institutions. The financial sector has to take into consideration the requirement of collecting necessary data for preventing money laundering, but at the same time, the protection of personal data has been taken into account.[154]

6. Conclusion

The GDPR is one of the most effective data protection legislation in the world. It sets stricter legal grounds for processing data without data subject's consent and ensures the data subject's right to access the data or withdraw the data. The GDPR affects the Member States of the EU and third-party countries who process the data through the EU. The wide application of the GDPR affected many sectors; one of them is financial sector and business-related authorities.

The study examined the legal issue concerning how financial crime data can be processed under the GDPR and analysed in the light of the 5th AML. The financial crime data is defined as data, collected by financial institutions of individuals who have a connection or are suspected of having contact with illicit financial actions. Financial crime data is important to collect and include a database for preventing financial crimes, for instance, money laundering. The banking industry is used to process large amounts of data in daily process and apply specific principles to detect abnormal appliance. However, the financial institutions have experienced changes after the GDPR came into force and had to consider new factors while processing the data and collecting it. The importance of data controller has arisen, legitimate interest and legal obligation to the process have strengthened the ability to process large amounts of data which the financial institutions have to consider in their process.

In the EU the 5th Anti-Money Laundering Directives is the current Directive fighting against financial crimes, specialised to the money laundering. It came into force in 2018 and

[153] See chapter 3.3.
[154] See chapter 3.3.

emphasised the importance of Know Your Customer principles in regard to money laundering. The KYC principles under the 5th AML implies requirements for financial institutions to collect the data based on the risk-based analysis in account to customer due diligence. Financial institutions have the responsibility to identify and manage the risks of money laundering, which is necessary for the system to prevent financial crimes and minimise the risk while entering into a new business relationship.

The problem is finding the balance between the necessary processing information for financial institutions and protecting personal data in regard to the GDPR. As mentioned in the GDPR, the processed data has to have a legitimate interest, legal obligation or agreement between the data controller and the data subject. Institutions are obligated to record the process of collecting data, and in case of data subject requesting the collected data, the controller has to give access to it. Furthermore, the data subject has the right to be erased, which means that the financial institution cannot keep record the information of the customer without legal obligation or legitimate interest. However, as found in the study, the GDPR is permissive to process the data in regard to prevent financial crimes, and most of the financial crimes or fraud fall under the scope of article 6 (1) (c) and 6 (1) (f) of the GDPR. The legal framework for financial crime data needs legal certainty and clearer guidance to reach full benefit in the financial sector.

7. Bibliography

7.1 Articles

Albrecht, J, P, 'How the GDPR will change the world' (2016) 2(287) Eur. Data Prot. L. Rev.

Chohan, U, W, 'The FATF in the Global Financial Architecture: Challenges and Implications.' (2019) Social Science Research Network

Dinev, T, 'Why would we care about privacy?' (2014) 23(2) European Journal of Information Systems <https://doi.org/10.1057/ejis.2014.1> accessed on 30 March 2019

European Union Agency for Fundamental Rights 'Handbook: Preventing unlawful profiling today and in the future - a guide' (2018) The European Union Agency for Fundamental Rights

European Union Agency for Fundamental Rights, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union – Volume II – Summary' (2018) The European Union Agency for Fundamental Rights

Gilbert, F, 'EU General Data Protection Regulation: What impact for Businesses Established Outside the European Union' (2016) 19(11) Journal of Internet Law <https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=115322774&site=ehost-live> accessed on 30 March 2019

Glynn, L, 'KYC vs Data Protection – The next compliance hurdle' (2016) Fenergo

Jackson, O, 'Many small firms are still unprepared for GDPR' (2018) International Financial Law Review

Malish, R, 'Financial Crime and Compliance under GDPR' (2018) NICE Actimize

Milaj, J, Kaiser, C, '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://doi-org.db.ub.oru.se/10.1093/idpl/ipx002> accessed 2nd May 2019

Miru, B, R, 'Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes' (2019) Poly & Globalization

Nance, M, T, 'The regime that FATF built: an introduction to the Financial Action Task Force' (2018) Crime, Law and Social Change

Tyson, J, E, 'International financial centres and development finance' (2019) ODI

7.2 Books

Corrales, Marcelo, Fenwick, Mark & Forgó, Nikolaus *New Technology, Big Data and the Law* (Springer 2017)

Cox, Dennis *Handbook of Anti-Money Laundering* (John Wiley & Sons 2014)

Horspool, Margot, Humphreys, Matthew & Wells-Greco, Michael *European Union Law* (9th edn, OPU 2015)

Nääv, Maria & Zamboni, Mauro *Juridisk metodlära* (2nd edn, Studentlitteratur 2018)

Voight, Paul & Bussche, Axel *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017)

7.3 Case-law

Case C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme' [2017] OJ C213/11

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

7.4 Conventions

Consolidated Version of the Treaty on European Union [2008] OJ C115/13

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1

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

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

Council Directive (EC) 2009/110 of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7

Council Directive (EC) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35

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

Council Directive (EC) 2018/1673 on combating money laundering by criminal law [2018] OJ L284/22

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

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

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

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 (Data Protection Directive) [2016] OJ L119/1

The Charter of Fundamental Rights of the European Union [2016] OJ C202/02

7.5 Opinions, Propositions and Recommendations

European Data Protection Supervisor, 'Formal comments of the EDPS on a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market' (2018) The EDPS

Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2018) The FATF Recommendations

Presidency of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach' (2012) Council of the European Union

The European Data Protection Supervisor, 'Annual Report 2018' (2018) Publications Office of the European Union

The European Data Protection Supervisor, 'EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC: Access to beneficial ownership information and data protection implications' (2017) The EDPS

7.6 Webpages

European Commission 'What is Personal Data?' *(EC Europa EU)* <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> accessed on 29 March 2019

European Union 'EU Law' (*Europa EU*, 27 February 2019) <https://europa.eu/european-union/law_en> accessed on 28 March 2019

Europol 'Economic Crime' *(Europol Europa EU)* <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime> accessed on 29 March 2019

Financial Action Task Force ‘Who we are’ *(FATF GAFI)* <http://www.fatf-gafi.org/about/> accessed on 29 March 2019