Master’s Thesis in EU Law
30 ECTS

Anti-Money Laundering and the Right to Privacy

A Study of Potential Conflicts between the Processing of Bank Information to Fight Crime and the Protection of Personal Data

Author: Louise Österberg
Supervisor: Senior Lecturer Maria Bergström
# Table of Contents

**Abbreviations** ........................................................................................................... v

**1 Introduction** ............................................................................................................... 1

1.1 Background .................................................................................................................. 1
1.2 Objectives .................................................................................................................... 2
1.3 Scope and Delimitations ............................................................................................. 2
1.4 Method and Sources ................................................................................................... 3
1.5 Outline ......................................................................................................................... 6

**2 Storing and Sharing Personal Data in the Bank Register** ........................................ 7

2.1 The Development of EU law on AML ........................................................................ 7
2.2 Purpose and Application of the AML Directives ...................................................... 8
2.3 General Obligations .................................................................................................... 9
   2.3.1 General Obligations to Collect and Store Information ...................................... 9
   2.3.2 General Obligations to Share Information ......................................................... 10
2.4 The Bank Register ..................................................................................................... 13
   2.4.1 Storing Information in the Bank Register .......................................................... 13
   2.4.2 Sharing Information in the Bank Register ......................................................... 15
2.5 Summary .................................................................................................................... 17

**3 Protection of Personal Data in the GDPR and the LED** .......................................... 18

3.1 Background and Application ...................................................................................... 18
3.2 Personal Data, the Controller and Principles of Data Protection .............................. 19
3.3 The Bank Register, the GDPR and the LED .............................................................. 21
   3.3.1 Storing and Sharing Personal Data in the Bank Register ................................ 21
      3.3.1.1 Lawfulness, Fairness and Transparency .................................................... 21
      3.3.1.2 Purpose Limitation .................................................................................. 22
      3.3.1.3 Data Minimisation .................................................................................. 24
      3.3.1.4 Accuracy .................................................................................................. 26
      3.3.1.5 Storage Limitation ................................................................................... 26
      3.3.1.6 Integrity and Confidentiality ................................................................... 27
3.4 Summary .................................................................................................................... 28
4 The Right to Protection of Personal Data and Private Life in the Charter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Introduction</td>
<td>29</td>
</tr>
<tr>
<td>4.2 Digital Rights Ireland and Tele2 Sverige AB</td>
<td>30</td>
</tr>
<tr>
<td>4.3 Application</td>
<td>32</td>
</tr>
<tr>
<td>4.4 Interference</td>
<td>33</td>
</tr>
<tr>
<td>4.5 Lawful Limitations: Legal Basis, Essence of the Right and Objective of General Interest</td>
<td>35</td>
</tr>
<tr>
<td>4.6 Proportionality</td>
<td>37</td>
</tr>
<tr>
<td>4.6.1 Appropriate</td>
<td>37</td>
</tr>
<tr>
<td>4.6.2 Is the Storing of Personal Data in the Bank Register Strictly Necessary?</td>
<td>37</td>
</tr>
<tr>
<td>4.6.2.1 Introduction</td>
<td>37</td>
</tr>
<tr>
<td>4.6.2.2 Link Between Data Subject and Criminal Activity</td>
<td>39</td>
</tr>
<tr>
<td>4.6.2.3 Retention Period</td>
<td>41</td>
</tr>
<tr>
<td>4.6.2.4 Security Standards</td>
<td>43</td>
</tr>
<tr>
<td>4.6.3 Is the Sharing of Personal Data in the Bank Register Strictly Necessary?</td>
<td>45</td>
</tr>
<tr>
<td>4.6.3.1 Introduction</td>
<td>45</td>
</tr>
<tr>
<td>4.6.3.2 Objective to Fight Serious Crime</td>
<td>46</td>
</tr>
<tr>
<td>4.6.3.3 Conditions for the Access</td>
<td>48</td>
</tr>
<tr>
<td>4.6.3.4 Prior Review and Supervision</td>
<td>49</td>
</tr>
<tr>
<td>4.6.3.5 Other Safeguards</td>
<td>52</td>
</tr>
<tr>
<td>4.7 Summary</td>
<td>54</td>
</tr>
</tbody>
</table>

5 Conclusion and Final Remarks

Bibliography
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>AMLD4</td>
<td>Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing</td>
</tr>
<tr>
<td>AMLD5</td>
<td>Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing</td>
</tr>
<tr>
<td>Charter</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit</td>
</tr>
<tr>
<td>GDPR</td>
<td>Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC</td>
</tr>
<tr>
<td>IBAN</td>
<td>International Bank Account Number</td>
</tr>
<tr>
<td>LED</td>
<td>Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA</td>
</tr>
<tr>
<td>MS</td>
<td>EU Member State(s)</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty of the European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty of the Functioning of the European Union</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety".¹

When the person, who most likely was Benjamin Franklin, wrote these words for the first time in 1755, he probably could not have guessed what significance they would have in society 260 years later.

Unlike people in 1755, almost everyone today uses electronic devices in their everyday life. For example, it is common today to pay with a card or smartphone instead of using cash. It is also possible to pay bills and transfer money to others within seconds using modern technology. This development has for many resulted in a more convenient lifestyle, but at the same time, this efficient system is also being used for illegal and harmful activities. Wire transfers and mobile payment is an efficient way to hide the illicit origin of proceeds or to collect funds for harmful activities, such as terrorist attacks. Cases like the Panama Papers and the September 11 attacks show what a major threat money laundering and terrorist financing pose to society and the financial system.

To keep society safe, the legislator has introduced different systems to prevent the use of the financial system for the purpose of money laundering and terrorist financing. In the European Union (EU), the most recent legislative measures in this area are AMLD5 on prevention of money laundering and terrorist financing², which amends AMLD4³, and Directive 2018/1673 on combating money laundering by criminal law⁴. The preventive measures are, in difference to the measures on criminal law, characterised by an obligation to know the people you do business with and what they do with their money. This is a procedure that entails processing of information about customers and their activities.⁵

---

¹ Pennsylvania Assembly: Reply to the Governor, 11 November 1755.
³ Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, (AMLD4).
⁴ Directive (EU) 2018/1673 on combating money laundering by criminal law.
⁵ See for example, chapter II of the AMLD4 on Customer Due Diligence (CDD) and amendments to this chapter in articles 1.6–1.14 of the AMLD5.
Surveillance to some extent could probably be acceptable, if it helps to prevent crime. However, the possibility to confine liberty by processing information cannot be unrestricted. That is why all EU citizens enjoy protection of personal data and privacy through the General Data Protection Regulation (GDPR)⁶, the Law Enforcement Directive (LED)⁷ and the Charter of Fundamental Rights of the European Union (Charter)⁸.

1.2 Objectives

It can be difficult to find the right balance between the fight against crimes and the protection of privacy. Since the preventive measures used to fight money laundering and terrorist financing centre around the processing of information about individuals, they can be particularly problematic. The objective of this thesis is to investigate potential conflicts between storing and sharing personal data in bank registers and the protection of privacy within the EU.

To meet this objective, the thesis will answer the following questions:

1. What obligations to store and share personal data in bank registers does EU law impose on the EU Member States (MS)?
2. What potential conflicts are there between these obligations and the protection of personal data in the GDPR and the LED?
3. What potential conflicts are there between these obligations and the right to protection of personal data and private life in the Charter?

1.3 Scope and Delimitations

This thesis will focus on the recent obligation for the MS to put in place a centralised and automated mechanism with information about payment and bank account holders within the MS (hereafter referred to as the bank register).⁹ Although financial actors have stored and shared information about their customers to prevent crime for a long time, the bank

---

⁶ Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (GDPR).
⁷ Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, (LED).
⁸ See specifically articles 7, 8 & 52 of the Charter.
⁹ Article 1.19 of the AMLD5.
register will introduce significant changes in the way this information is stored and shared. These changes could entail new challenges from a privacy perspective which this thesis aim to examine. It should be noted that storing and sharing of information are the only two types of processing that this thesis will analyse.

The bank register is regulated in AMLD4 and AMLD5. These two AML Directives complement Directive 2018/1673 that aims to combat money laundering by criminal law, but they serve different purposes. Whilst Directive 2018/1673 aim to create a harmonised view of money laundering as a crime, the AML Directives aim to harmonise measures that prevent the use of the financial system for such crimes. The bank register is a preventive measure and therefore regulated in AMLD4 and AMLD5. Directive 2018/1673 does not regulate the bank register and will, therefore, not be analysed further.

AMLD4 and AMLD5 aim to prevent both money laundering and terrorist financing. To avoid repetition, the thesis will use the term Anti-Money Laundering (AML) to refer to both the fight against money laundering and terrorist financing. If there is a reason to separate the two terms, it will be stated.

EU law correlates with national and other international law but can also be seen as an independent legal system. This thesis will focus on potential conflicts within the EU independent legal system and will therefore only study EU legal acts. One exception to this rule is the case law from the European Court of Human Rights (ECtHR) on the interpretation of the European Convention on Human Rights (ECHR), as this also can be used to interpret the Charter. National law will occasionally serve as examples to highlight some of the problems at the EU level.

1.4 Method and Sources

As clarified in the previous section, this thesis will focus on EU law as an independent legal system. There are two levels of law in EU law; primary and secondary. Secondary law that does not comply with primary law may be annulled. Primary law consists of the Treaty of the European Union (TEU), Treaty of the Functioning of the European Union (TFEU) and the Charter, which all have equal standing. Regulations and

11 Article 1.1 of the AMLD4.
14 Streinz, European Legal Methodology, p 153; Barnard & Peers, European Union Law, p 104.
Directives are part of the EU secondary law. A regulation is “binding in its entirety and directly applicable in all MS”. Directives are different from regulations as they often are not directly applicable, but have to be implemented in national law to give effect in the MS. Although directives only are binding to the result and not the measure, they tend to be very detailed which means that the MS do not have much discretion in practice.

The legal acts of importance in this thesis are mainly part of secondary law. The relevant AML legislation will consist of two Directives, namely AMLD4 and the AMLD5. AMLD4 still constitutes the main legal act, although AMLD5 has amended it substantially, e.g. by introducing the bank register. The two AML Directives thus apply parallel to each other and both regulate the bank register. The data protection law that governs the AML measures consist of both a regulation and a directive. That the data protection law consists of two different kinds of legal acts mainly affects their application on the national level and will therefore not affect the analysis in this thesis. Since Directives usually are detailed, this difference probably will not affect the interpretation of the frameworks either.

Apart from analysing potential conflicts between the AML Directives and secondary law, this thesis will also examine potential conflicts between the secondary law and the Charter in order to fulfil its purpose. The primary and secondary law is related both in the sense that the secondary law can be annulled if it does not comply with primary law and that the secondary law therefore should be interpreted in a way that is compliant with primary law.

When this thesis interprets EU law, it considers foremost the purpose of the act and its context. This comes from the effet utile-doctrine, which ensures the effectiveness of EU law and that the purpose of an act is attained as far as possible. The recitals in the beginning of an act will be used to understand the purpose of the act and its provisions. According to the acte clair rule, the wording of an act also is of importance particularly

---

15 Article 288 subpara 2 of the TFEU.
16 Barnard & Peers, European Union Law, p 100.
17 Article 288 subpara 3 of the TFEU; Barnard & Peers, European Union Law, p 100.
18 Recital 1 of the AMLD5.
19 Riesenhuber, Interpretation of EU Secondary Law, p 256.
20 Riesenhuber, Interpretation of EU Secondary Law, pp 256–257.
21 Riesenhuber, Interpretation of EU Secondary Law, p 252.
22 Riesenhuber, Interpretation of EU Secondary Law, p 249.
if it is unambiguous. Acte clair is easier to apply to primary law than to secondary law, because the wording in secondary law more often is ambiguous. The Court of Justice of the European Union (CJEU) also uses the wording, the legal context and the objective of a provision when interpreting EU law.

Apart from the legal acts themselves, the case law of the CJEU is essential as it has an important role for the interpretation and application of EU Law. In particular, the third research question will be answered by analysing the case law of the CJEU. There are no cases from the CJEU concerning the bank register. Therefore, two cases concerning processing of information relating to telecommunication will be used in the analysis instead. These cases have been chosen as the circumstances are similar to the requirements of the bank register, which will be clarified in relation to that analysis.

The case law of the ECtHR on the interpretation of the ECHR will also be important for the interpretation of the Charter. The EU is not a party to the convention itself, but the rights in the ECHR have for a long time been regarded as principles within EU law and has, thereby, affected its application. These principles were codified as its own set of rights in the Charter. When the ECHR and the Charter regulate rights that overlap, the scope of those rights shall be the same in both frameworks. The interpretation of article 8 of the ECHR on the right to respect for private and family life can therefore assist in the interpretation of articles 7 and 8 of the Charter in the analysis of this thesis.

The EU legal system also consist of independent authorities. One such independent authority is the European Data Protection Supervisor (EDPS) which shall ensure that data protection rules are respected by Union institutions and advising them on all matters concerning data protection. The EDPS was consulted in relation to the proposal of AMLD5 regarding possible problems relating to data protection. This opinion of the

---

24 Riesenhuber, European Legal Methodology, p 255.
25 Reichel, Juridisk metodlära, p 122.
26 Article 19.1 of the TEU.
28 Article 52.3 of the Charter.
29 Articles 52.2 & 52.3 of Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of the personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001.
EDPS is not binding but will be used to support arguments in the thesis.\textsuperscript{31} Doctrine relevant for this thesis is limited, but it will occur occasionally to support arguments in the analysis.

1.5 Outline

The following section 2 will introduce the legislation for AML within the EU and the provisions that are relevant for the analysis. It will begin to provide a broad background that will serve as a basis to understand AML legislation and then give a more detailed description of the regulation of the bank register, thus answering the first research question. It will also highlight the differences between processing of information in and outside of the bank register.

The second research question will be answered in section 3. That section will study relevant provisions of data protection in the GDPR and the LED, to see how these affect the processing of information in the bank register and potential conflicts between the frameworks. Section 4 will answer the third research question, namely if there also are any potential conflicts between the bank register and the rights to protection for personal data and private life in the Charter. The CJEU has laid down some criteria in their case law on how these rights should be interpreted, which will guide the analysis in this section.

The reason for the division between section 3 and 4 is that the bank register could be in conflict with the provisions in the GDPR and the LED by themselves. At the same time, the bank register together with the data protection in the GDPR and the LED could constitute a breach of the Charter. It is therefore interesting to look at these conflicts separately. To some extent these sections overlap, something that has been solved with cross-references. Lastly, there will be a conclusion in section 5 that presents the findings of the thesis, accompanied with some final remarks.

\textsuperscript{31} Article 288 subpara 5 of the TEUF.
2 Storing and Sharing Personal Data in the Bank Register

2.1 The Development of EU law on AML

Money laundering is the process of making profits from criminal activity appear legitimate, for example by making money earned from drugs or trafficking usable for ordinary and legal purposes.\(^{32}\) It is therefore at the core of many serious and global crimes.

The first AML Directive\(^ {33}\) was adopted in 1991. It contained both elements of criminalisation and prevention of money laundering, and thereby became the first comprehensive framework for AML within the EU.\(^ {34}\) Since then, AML legislation within the EU has developed parallel with international progress, particularly from documents of the Financial Action Task Force (FATF).\(^ {35}\) FATF is an inter-governmental body, established to improve AML measures, that has developed a series of non-binding recommendations that are recognised as the international standard for AML.\(^ {36}\) After the September 11 attacks, combating financing of terrorism became an additional and equally important purpose of the AML legislation.\(^ {37}\) This was officially introduced through the third AML Directive\(^ {38}\) which also introduced other significant changes such as the risk-based approach.\(^ {39}\) The most recently adopted Directive is AMLD5, which amends AMLD4 and shall be implemented by 2020.\(^ {40}\) AMLD4 and AMLD5 are adopted on the basis of article 114 of the TFEU, which is meant to ensure the functioning of the internal market. There is a possibility for the MS to impose stricter rules to fulfil the purpose of the AML Directives, as long as this is within the limits of EU law.\(^ {41}\)

The following sections will first discuss more general provisions in AMLD4 and AMLD5 which still are important in the analysis. There will then be a more detailed

\(^{32}\) Article 1.3 of the AMLD4.


\(^{34}\) Mitsilegas & Gilmore, \textit{The EU legislative Framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards}, pp 119–120.

\(^{35}\) Mitsilegas & Gilmore, \textit{The EU legislative Framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards}, p 120.

\(^{36}\) FATF, “About”.


\(^{38}\) Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

\(^{39}\) Recital 10 & article 8 of Directive 2005/60/EC.

\(^{40}\) Recital 53 & article 4 of the AMLD5.

\(^{41}\) Article 5 of the AMLD4.
description of provisions regulating the bank register and what changes the bank register entails.

2.2 Purpose and Application of the AML Directives

The overall purpose of the AML Directives is to “prevent the use of the Union’s financial system for the purpose of money laundering and terrorist financing”. Preventive measures are important complements to the development of criminal law on AML. They cannot only be efficient in detecting, but also in deterring, crime. It is important to regulate preventive measures at the EU level in order to protect the common financial system.

Part of the definition of money laundering is that the proceeds have derived from criminal activity. The term criminal activity consists of a couple of crimes, including terrorist offences, drug trade, and tax crimes when they are punishable by detention for a certain period of time. Hence, the AML Directives target money laundering of gains from these crimes only. Terrorist financing is defined in the AML Directives as the collection of funds for a terrorist offence. The AML Directives apply to obliged entities which include several actors like credit and financial institutions.

Although AML is the only clear policy goal of the AML Directives, there have been arguments that the amendments in AMLD5 also indicate other policy goals, such as tax evasion. This means that not only laundering of gains from tax evasion is targeted, but also tax evasion as such. The provisions regarding the bank register contributes to this interpretation, something that will be further discussed in section 2.3.2.

42 Article 1.1 of the AMLD4.
43 Recital 1 of the AMLD4.
44 Recital 4 of the AMLD5.
45 Recital 2 of the AMLD4.
46 Article 1.3 of the AMLD4.
47 Article 3.4 of the AMLD4; article 1.2 of the AMLD5.
48 Article 1.5 of the AMLD4.
49 Article 2.1 of the AMLD4.
50 EDPS Opinion 1/2017, paras 18 & 29.
2.3 General Obligations

2.3.1 General Obligations to Collect and Store Information

The risk-based approach is central in the AML legislation. This approach means that the obliged entities shall identify the risk for money laundering in their business, taking into account e.g. the customers, geographical areas and type of products. AML policies and procedures shall then be based on this risk assessment.\(^{51}\)

The risk-based approach was partly introduced to stop the overload of reports of suspicious transactions that reduced investigation capacity. Another reason was to give the obliged entities a flexibility to deal with complex problems. Thirdly, the approach gave the obliged entities the responsibility to implement AML procedures that best suited their businesses. This shift of responsibilities shows the trend within AML to move regulatory functions from public authorities to private actors, with the aim to make the private actors more active in the prevention and thus make the prevention more efficient.\(^{52}\)

The risk with a certain business relationship affects the amount and type of information that shall be collected about a customer, in the process referred to as customer due diligence (CDD).\(^{53}\) CDD shall be conducted, for example, when a business relationship is established or when carrying out transactions of certain amounts both electronically and with cash.\(^{54}\) When the risk is considered low, a simplified CDD may be conducted, and vice versa.\(^{55}\) Anonymous accounts are forbidden.\(^{56}\) Some CDD measures that always shall be carried out are verification of the identity of the customer, as well the beneficial owner, and the purpose of the business relationship.\(^{57}\) The obliged entities shall also monitor the business relationship, including transactions, to see that this in line with the information they have about the customer.\(^{58}\)

All obliged entities are required to hold information about the beneficial owner as part of the CDD.\(^{59}\) The beneficial owner is a person that ultimately owns or controls a legal entity, for example by owning a certain percentage of the shares or voting rights.\(^{60}\)

---

\(^{51}\) Article 8 of the AMLD4.
\(^{53}\) Article 13.2 of the AMLD4.
\(^{54}\) Article 11 of the AMLD4.
\(^{55}\) Articles 15 & 18 of the AMLD4; article 1.10 of the AMLD5.
\(^{56}\) Article 1.6 of the AMLD5.
\(^{57}\) Article 13 of the AMLD4; article 1.8 of the AMLD5.
\(^{58}\) Article 13.1.d of the AMLD4.
\(^{59}\) Article 30.1 of the AMLD4; article 1.15 of the AMLD5.
\(^{60}\) Article 3.6 of the AMLD4; article 1.2 of the AMLD5.
This information is important as it makes it harder for criminals to hide behind a corporate structure.\textsuperscript{61} In order to further enhance transparency, the information about beneficial owners shall also be held in a centralised register, which to different degrees is open to authorities as well as the general public.\textsuperscript{62}

The information included in the CDD shall be retained for five years after the business relationship has ended.\textsuperscript{63} This retention period has been the same since the First AML Directive, which then considered the period necessary in order for the information to be used as evidence in investigations.\textsuperscript{64} According to AMLD4, the limit is fixed to five years for reasons of data protection and legal certainty.\textsuperscript{65} After the retention period has ended the information shall be deleted.\textsuperscript{66} The information may, however, be retained for an additional period of max five years after the first retention period expires, if this is considered necessary for AML.\textsuperscript{67}

Specific safeguards should be put in place to protect the data from unlawful access.\textsuperscript{68} The individuals whose data is being processed also have a possibility to access the information about themselves although this can be limited in relation to suspicious transactions in accordance with data protections rules.\textsuperscript{69}

Collecting and storing information is a significant part of AML preventive measures, even without the requirement to keep it in a bank register. Before and parallel to the bank register, the obliged entities store this information within their companies.\textsuperscript{70} They entities have to share the information of the CDD under certain circumstances, which will be described in the following section.

2.3.2 General Obligations to Share Information

Every MS shall have an Financial Intelligence Unit (FIU) that works to “\textit{prevent, detect and effectively combat money laundering and terrorist financing}”.\textsuperscript{71} The FIU shall be operationally independent and responsible for receiving and analysing information

\textsuperscript{61} Recital 14 of the AMLD4.
\textsuperscript{62} Recital 14 & article 30.3 of the AMLD4; article 1.15 of the AMLD5.
\textsuperscript{63} Article 40.1 of the AMLD4; article 1.25 of the AMLD5.
\textsuperscript{64} Article 4 of Council Directive 91/308/EEC.
\textsuperscript{65} Recital 44 of the AMLD4.
\textsuperscript{66} Article 40.1 subpara 2 of the AMLD4.
\textsuperscript{67} Article 40.1 subpara 2 of the AMLD4.
\textsuperscript{68} Recital 44 of the AMLD4.
\textsuperscript{69} Recital 46 of the AMLD4.
\textsuperscript{70} Article 40 of the AMLD4.
\textsuperscript{71} Article 32.1 of the AMLD4.
relating to suspicions of money laundering.\textsuperscript{72} Obliged entities shall report any suspicious transactions to the FIU and in such cases provide the FIU directly with all necessary information.\textsuperscript{73} An obliged entity is not allowed to carry out a suspicious transaction or inform the suspect or a third-party that there is an ongoing investigation.\textsuperscript{74} The obliged entities shall, however, inform a new customer that information about them will be processed under the AML Directives.\textsuperscript{75}

To fulfil its purpose, the FIU shall also be able to request information from any obliged entity and forward the information to other competent authorities.\textsuperscript{76} A report of suspicion is not needed for the FIU to request information, but a request to another competent authority has to be based on sufficiently defined conditions.\textsuperscript{77} What those conditions are, is not further defined in the AML Directives. An FIU shall also be able to request and respond to requests for information from other competent authorities within the MS when it is needed to prevent money laundering, terrorist financing or associated predicate offences.\textsuperscript{78}

It is not defined in the AML Directives which authorities constitute \textit{competent authorities}. This makes it possible for any national authority that would be involved in fulfilling the purpose of AML to request information. It is a likely legal construction, as the set-up of competent authorities can be different in different MS, like the set-up of FIUs.\textsuperscript{79} This conclusion is also supported by the fact that the MS shall report a list of competent authorities to the European Commission, in order to facilitate the cooperation between those authorities in different MS. \textsuperscript{80} The MS can then implement the AML Directive in a way that suits their particular system and identify the relevant competent authorities in it. It should be noted that the definition of competent authorities is not the same as the definition in the GDPR and the LED, which will be discussed in section 3.1. A competent authority can essentially only refuse to share information with other competent authorities if it can impede an ongoing investigation.\textsuperscript{81}

\textsuperscript{72} Article 32.3 of the AMLD4.
\textsuperscript{73} Article 33 of the AMLD4; article 1.21 of the AMLD5.
\textsuperscript{74} Articles 35.1 & 39.1 of the AMLD4.
\textsuperscript{75} Article 41.3 of the AMLD4.
\textsuperscript{76} Article 32.3 of the AMLD4; article 1.18 of the AMLD5.
\textsuperscript{77} Recital 17 & article 1.18 of the AMLD5.
\textsuperscript{78} Article 32.4 of the AMLD4.
\textsuperscript{79} Recital 16 of the AMLD5.
\textsuperscript{80} Article 1.30 of the AMLD5.
\textsuperscript{81} Article 1.32 of the AMLD5.
In relation to competent authorities, there is one authority whose role in AML seems to be particularly emphasised in AMLD5. That is tax authorities.\(^{82}\) In regard to national cooperation, tax authorities are also mentioned separately, as one authority that the MS shall ensure have effective mechanisms to fight money laundering and terrorist financing.\(^{83}\) In this context, tax authorities are mentioned in addition to competent authorities, although they possibly could constitute competent authorities as well. This division between the two, indicates an emphasise by the legislator on the role of tax authorities in AML. Giving the tax authorities access to information strengthens their role in AML measures but it can also lead to conflicts with data protection law. This emphasise also indicates what was previously stated in section 2.2 that tax evasion has become a policy goal of AML in itself, which will be discussed further in section 3 and 4.

The cooperation between FIUs in different MS is also important, especially since money laundering and terrorist financing are international crimes.\(^{84}\) MS shall ensure that the FIUs exchange relevant information across borders within the EU, both spontaneously and upon request, for the purpose of AML or related predicate offences.\(^{85}\) The FIU to which the request is made shall respond in a timely manner and use the same resources as it would for a request within the MS.\(^{86}\) Such a request could be denied if the exchange would be contrary to national fundamental principles that have been specified.\(^{87}\) If an FIU wants to request information from an obliged entity in another MS, they must go through the FIU in that MS.\(^{88}\) The MS may also put some restrictions on the use of the information that the receiving FIU must comply with.\(^{89}\) The MS have had some trouble exchanging information due to different definitions of predicate offences such as tax crimes.\(^{90}\) Different definitions should, however, not limit the exchange across borders.\(^{91}\)

Another problem for the exchange of information between different MS is that the FIUs have different forms. These differences should not come in the way of the exchange of information though, and the FIUs should still cooperate to the greatest extent possible.\(^{92}\) Because of these different characters, the FIUs might follow different rules for

\(^{82}\) Recital 44 of the AMLD5.
\(^{83}\) Article 1.31 of the AMLD5.
\(^{84}\) Recital 54 of the AMLD4.
\(^{85}\) Article 53.1 of the AMLD4; article 1.33 of the AMLD5.
\(^{86}\) Article 53.2 of the AMLD4; article 1.33 of the AMLD5.
\(^{87}\) Article 53.3 of the AMLD4.
\(^{88}\) Article 53.2 of the AMLD4; article 1.33 of the AMLD5.
\(^{89}\) Article 54 of the AMLD4.
\(^{90}\) Recital 18 of the AMLD5.
\(^{91}\) Article 1.36 of the AMLD5.
\(^{92}\) Article 52 of the AMLD4; recital 16 of the AMLD5.
data protection.\textsuperscript{93} This will be discussed further in section 3.1. The FIUs shall also exchange information with FIUs in countries outside the EU, with regard to EU law, including EU data protection law.\textsuperscript{94}

The obliged entities, FIUs and competent authorities shall also have secure and confidential channels for the sharing of information to FIUs and other competent authorities.\textsuperscript{95} Furthermore, the MS should require safeguards for the security of data and should determine which persons, categories of persons or authorities should have exclusive access to it.\textsuperscript{96} Other national law requiring confidentiality should not hinder an exchange of confidential information according to the AML Directives.\textsuperscript{97} These measures to ensure confidentiality should all work to ensure that the information is shared with as few people as possible.

This section has introduced what the general rules for storing and sharing is in relation to AML information, many which exist parallel to the bank register. In the next section, the bank register will be further introduced.

\section*{2.4 The Bank Register}

\subsection*{2.4.1 Storing Information in the Bank Register}

As stated in the beginning, this thesis will focus on the bank register that is regulated through AMLD4 and AMLD5. The requirement that is laid down by the two AML Directives is that each MS shall put into place a centralised automated mechanism, such as a register or electronic data retrieval system. This mechanism shall allow for the identification of any natural or legal person holding or controlling a payment or bank account and safe-deposit boxes within the territory of the MS. For the bank and payment account, the register shall include the International Bank Account Number (IBAN), date of opening and closing, name of the holder and controller and the beneficial owner as well as other identification data, such as a personal identification number. For the safe-deposit boxes, the register must also include the name of the lessee and identification number, or similar, as well as the duration of the lease. Hereafter, the thesis will only refer to payment accounts as a name for all accounts and safe-deposit boxes. When it is

\textsuperscript{93} Mohamed, \textit{Legal Instruments to Combat Money Laundering in the EU Financial Market}, p 72.
\textsuperscript{94} Recital 58 of the AMLD4.
\textsuperscript{95} Article 42 of the AMLD4; article 1.30.b of the AMLD5.
\textsuperscript{96} Recital 44 of the AMLD4.
\textsuperscript{97} Article 1.32 of the AMLD5.
necessary to separate these terms, this will be stated. As the person that is controlling the account should be included in the bank register, information to identify the guardians for children and adults under guardianship will probably be included in the register.\textsuperscript{98}

The information that have to be included in the bank register was already stored at each obliged entity before the bank register as part of their CDD measures. Identification, for example, is always required as a CDD measure.\textsuperscript{99} The difference now is that this information also will be stored in the bank register, thus stored in an additional and different way. The information that all banks have collected about an individual will now be available at the same place, allowing for an overview of that individual’s economic engagements. It is this difference in storing the information that could entail new challenges from a privacy perspective.

Other information that the MS deem essential to fulfil the obligation under the AML Directives, may also be included in the bank register.\textsuperscript{100} Only the minimum data necessary for carrying out investigations of this kind should be included though.\textsuperscript{101} What is to be considered \textit{essential or necessary} is not further defined. The AML Directives do not make a difference between the people that the information concerns, for example on the basis of risk which the CDD measures are based on. Stepping away from the risk-based approach also a difference between the bank register and other AML measures.

The information in the bank register shall be stored there for the same retention period of five years as the CDD information at the obliged entities.\textsuperscript{102} The end of a business relationship, would in this context probably mean when a payment account is closed. Although the way of storing the information has changed, the retention period is the same as for CDD stored outside the register. This means that the retention period for the information in the bank register also can be extend for an additional five-year period. The information in the bank register should be possible to extend on a general basis though, not requiring case-by-case decisions.\textsuperscript{103} This urge for extension on a general basis is a difference with storing information in the bank register.

\textsuperscript{98} Article 1.19 of the AMLD5.
\textsuperscript{99} Article 13 of the AMLD4; article 1.8 of the AMLD5.
\textsuperscript{100} Article 1.19 of the AMLD5.
\textsuperscript{101} Recital 21 of the AMLD5.
\textsuperscript{102} Article 40.1 of the AMLD4; article 1.25 of the AMLD5.
\textsuperscript{103} Recital 21 of the AMLD5.
2.4.2 Sharing Information in the Bank Register

The information in the bank register shall be “directly accessible in an immediate and unfiltered manner to national FIUs”. This means that the FIUs no longer have to turn to each obliged entity to request information and wait for their reply as they have to without a bank register. Instead they can access the information directly in the bank register. This efficient process was actually the main reason for introducing the bank register as delayed access to information slowed down investigations. To highlight the differences that the bank register entail, the situation in Sweden, which does not have a bank register in place yet, will serve as an example.

In Sweden now, without a bank register, the FIUs have to contact every bank separately to request information about a particular person. Since the FIU does not know beforehand where a suspected person has their payment account, they have to request information from each potential financial entity separately. This is usually done through an “umbrella-demand”, meaning that the FIU send out a general request to several actors.

This procedure is time-consuming and costly. It is an administrative burden for both the financial actor and FIU to handle these requests individually. Due to this burden, the FIU do not have the possibility to send the request to all financial actors, but only the main actors where it is more likely that an individual has an account. It is therefore possible that some accounts are missed, and it is also easy for the criminal to avoid scrutiny by choosing smaller actors. In this way, one can even argue that the current legislation does not fulfil its AML-purpose in this aspect. With the bank register, it will be easier for the FIU to get an overview of what financial actors a person is connected to and they would then know who they should turn to for more information.

Without a bank register, each obliged entity have to handle the requests from the FIU and make an assessment of whether the information should be handed out or not, although it is likely that they mostly hand out the information as they have such a strong obligation to do so. As the FIU now has direct access in an immediate and unfiltered manner, the decision to access information in the register would solemnly take place within the FIU. This could be problematic from a privacy perspective, although it already

---

104 Article 1.19 of the AMLD5.
105 Recital 20 of the AMLD5.
106 Promemoria, Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv, p 54.
107 Promemoria, Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv, p 55.
108 Article 33.1 of the AMLD4; article 1.21 of the AMLD5.
is easy to receive information from an obliged entity. This will be discussed further in section 4.6.3.4.

Other national competent authorities shall also have access to the information in the bank register for fulfilling their obligations under the AML Directives.\textsuperscript{109} Before the bank register, the competent authorities went through the FIU to receive information. Now, it seems as if it instead is possible for them to access the bank register directly to some extent. All access to the bank register should be on a need-to-know basis.\textsuperscript{110} The conditions on which the information in the register can be accessed has not changed from the necessary criterion before, although the way of accessing the information is different.

The FIUs shall also be able to pass the information to other FIUs in other MS as well as third-countries in accordance with the general rules of sharing.\textsuperscript{111} This is something that has not in itself changed by the requirement of the bank register, although it can be affected by how the information initially is shared. The potential issues with the different forms of FIUs and definitions of tax crime is also relevant for the bank register as the information in the bank register can be shared that way.

The bank register must also ensure security and confidentiality when sharing information in the register in accordance with the same rules for general obligations. In this regard, the bank register might by its design be more secure than the measure before. Actually, bank registers were encouraged already in AMLD4 because it could be a secure and confidential way of sharing information to authorities.\textsuperscript{112} One reason for this could probably be that the FIUs do not have to contact each entity but only the ones that are relevant.\textsuperscript{113} This means that less entities will find out about the suspicions, which protects the privacy of the data subject.

Another form of security measure that apply to both the bank register and other processing is that they should respect EU data protection law.\textsuperscript{114} The MS shall also assess data protection concerns in relation to their implementation of the AML Directives.\textsuperscript{115} These and other data protection rules will be further discussed in section 3.

\textsuperscript{109} Article 1.19 of the AMLD5.
\textsuperscript{110} Recital 21 of the AMLD5.
\textsuperscript{111} Article 53 of the AMLD4; articles 1.19 & 1.33 of the AMLD5.
\textsuperscript{112} Recital 57 of the AMLD4.
\textsuperscript{113} Promemoria, Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv, pp 54–55.
\textsuperscript{114} Recital 42 of the AMLD4; recital 38 of the ALMD5.
\textsuperscript{115} Article 7.1 of the AMLD4.
2.5 Summary

In sum, the MS are obliged to set-up a bank register that must store certain information that allows for identification but also that gives the MS an opportunity to include more information. This information will allow for a good overview of an individual’s economic engagements, that was not possible before the bank register. Furthermore, the bank register will allow for this information to be shared more directly and rapidly with different authorities that also have different purposes. In the following section it will be investigated how these obligations relate to data protection rules.
3 Protection of Personal Data in the GDPR and the LED

3.1 Background and Application

The EU adopted its first Directive on data protection in 1995 to harmonise the legislation in the area and make the protection of personal data more equal in the MS.\textsuperscript{116} This Directive 95/46/EC did not, however, cover processing of personal data by authorities for law enforcement.\textsuperscript{117} To fill this gap in the legislation, the EU adopted Council Framework Decision 2008/977/JHA.\textsuperscript{118} Both of these acts were repealed and replaced through an extensive reform in 2016 that consisted of the GDPR and the LED. The reform in 2016 aimed to further harmonise the protection of personal data and rules regarding the free movement of such data.\textsuperscript{119}

The GDPR applies to the general processing of personal data.\textsuperscript{120} The processing of personal data for the purpose of AML shall be considered a matter of public interest in the GDPR, and it therefore applies to the AML Directives.\textsuperscript{121} As mentioned earlier, the GDPR as a regulation is directly applicable in all MS and can be invoked by a natural person in a domestic court.

The GDPR contains general rules for processing of personal data, whilst the LED lays down the rules for processing of personal data in the law enforcement context.\textsuperscript{122} The LED solely applies when a competent authority processes data for the purpose of, for example, prevention, investigation or detection of criminal offences.\textsuperscript{123} In these cases, the LED applies instead of the GDPR and only these rules have to be complied with.\textsuperscript{124} The AML Directives should be applied in a way that leaves the provisions in the LED in force.\textsuperscript{125} Considering the special nature of law enforcement the LED allows for a bit more flexibility to process personal data, although it to a large extent follows the principles in the GDPR.

\textsuperscript{116} Recitals 7 & 8 of 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.
\textsuperscript{117} Article 3.2 of Directive 95/46/EC.
\textsuperscript{118} Article 1 of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
\textsuperscript{119} Article 1 of the GDPR; recital 15 of the LED.
\textsuperscript{120} Article 1 of the GDPR.
\textsuperscript{121} Recital 42 & article 1 of the AMLD4; recital 38 & article 1.26 of the AMLD5.
\textsuperscript{122} Recital 19 of the GDPR; recital 9 of the LED
\textsuperscript{123} Recital 1.1 of the LED.
\textsuperscript{124} Recital 19 of the GDPR; Quintel, \textit{Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules}, p 36.
\textsuperscript{125} Recital 42 of the AMLD4; recital 40 of the AMLD5.
As brought up earlier, the set-up of the FIUs in the MS differ and this can affect the possibility for them to share information with each other, also in regard to the information in the bank register. This is because the different nature of the FIUs make it hard to determine if it is the rules in the GDPR or the LED that shall apply, and that both frameworks can apply to the different parties in an exchange. Not only is this a problem in the exchange between FIUs in different MS, but for the analysis in this thesis, this can be interesting as it determines what rules regulate the access to the information in the bank register within the MS. Although the FIUs pursue the same purpose, they could process information in accordance with different standards.

As the GDPR applies to processing in general and the LED only under particular circumstances, it is the criteria for the application of the LED that determines what framework should be applied. One of these criteria is that the processing must be carried out by a competent authority. Due to the different nature of the FIUs in different MS, they might sometimes be considered competent authorities and sometimes not. There is therefore a possibility that both the GDPR and the LED can apply to the processing of the information in the bank register. Consequently, both the LED and the GDPR will be analysed in this thesis and problems relating to their differences will be discussed. When the rules in the frameworks differ that will be stated.

3.2 Personal Data, the Controller and Principles of Data Protection

Personal data is any information that relates to an identified or identifiable natural person. This definition is the same in the GDPR, the LED and the Charter. Examples of personal data given in the data protection laws are; name, identification number or information relating to an individual’s economic identity. This information is all required to be available in the bank register. The aim of including the information in the bank register is to allow for identification. As identification is the core criterion of personal data, this also indicates that the information in the bank register constitutes such
data. The consequence of fulfilling this definition is that the provisions in the GDPR and the LED will be relevant for the processing of the information.\textsuperscript{132} The information will hereafter be referred to as personal data. An individual whose data is being processed is referred to as the data subject.\textsuperscript{133}

The data protection laws make a difference between the controller and the processor. The controller is the entity that determines the purpose and the means of the processing.\textsuperscript{134} It shall be responsible for compliance with data protection principles.\textsuperscript{135} A processor is simply an entity that process data on behalf of the controller.\textsuperscript{136} It is not specified in the AML Directives who is the controller or the processor of the bank register. That ought therefore to be something that the MS can decide for themselves. Regarding the access, naturally each authority will be responsible for their own access as they then determine when and why the data is processed. For the general storing of the information, it could be more difficult to determine who the controller should be.

Who the controller is can depend on the set-up of the bank register. AMLD5 allows for both central registers and central data retrieval systems or having both.\textsuperscript{137} If the set-up is a central retrieval system, the controller might be the obliged entities for the storing whilst the competent authorities are controllers for their access. If a central register is chosen though, there should be a separate controller for this register. It is hard to determine who would be the most suitable controller in such a case. One possibility is the FIUs as they have an unfiltered access to the information, although they have to follow the legal provisions that determines the purpose of the storing. That the controller is difficult to identify is problematic as it becomes unclear who should be held accountable for complying with data protection rules. The EDPS also emphasised the importance of identifying the controller in its opinion on the AMLD5.\textsuperscript{138}

The data protection principles are brought up in the beginning of the GDPR and then codified in the sections in the GDPR and gives conditions for them to be exempted. The data protection principles are: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and

\begin{itemize}
  \item Article 1.1 of the GDPR; article 1.1 of the LED.
  \item Article 4.1 of the GDPR; article 3.1 of the LED.
  \item Article 4.7 of the GDPR; article 3.8 of the LED.
  \item Article 5.2 of the GDPR; article 4.4 of the LED.
  \item Article 4.8 of the GDPR; article 3.9 of the LED.
  \item Article 1.19 of the AMLD5.
  \item EDPS Opinion 1/2017, para 66.
\end{itemize}
confidentiality.\textsuperscript{139} As stated, the LED is to a large extent based on these principles and the definitions in the GDPR, although it considers the specific nature of the law enforcement context.\textsuperscript{140} It will be stated when the rules in the frameworks differ.

3.3 The Bank Register, the GDPR and the LED

3.3.1 Storing and Sharing Personal Data in the Bank Register

3.3.1.1 Lawfulness, Fairness and Transparency

Maybe the most fundamental principle is that of lawfulness. The processing is lawful if it is carried out on one of the grounds in article 6 of the GDPR or carried out for the purpose of article 1.1 of the LED.\textsuperscript{141} As stated above, the processing of information for the purpose of the AML Directives should be considered a public interest in the GDPR.\textsuperscript{142} It is likely that the purpose of the AML Directives also fulfil the purpose of the LED, when it concerns competent authorities according to that Directive, as AML is a way to prevent criminal offences. The bank register does not therefore seem problematic in this regard.

Fairness and transparency concern the right of the data subject to know when and for what purpose their data is being processed.\textsuperscript{143} As stated in section 2.3.2, the data subject should be informed that the data will be processed for AML purposes. As this should be done at the initial collection, the obliged entities would have to add to their routines that the data will be processed in the bank register.\textsuperscript{144} This principle also include a right to access for the data subject, not only to the actual information stored but also a notification that when the data is being processed.\textsuperscript{145} This right can be restricted if that access can impede an ongoing investigation.\textsuperscript{146} In the AML Directives, the data subject should be notified only when such a notification cannot impede an investigation.\textsuperscript{147} The data subjects will then have the possibility to seek a judicial remedy as data protection

\begin{itemize}
\item \textsuperscript{139} Article 5 of the GDPR.
\item \textsuperscript{140} Article 4 of the LED.
\item \textsuperscript{141} Article 8.1 of the LED.
\item \textsuperscript{142} Recital 42 & article 1 of the AMLD4; recital 38 & article 1.26 of the AMLD5.
\item \textsuperscript{143} Recital 39 & articles 5.1.a & 12–15 of the GDPR; article 13 of the LED.
\item \textsuperscript{144} Article 13 of the GDPR.
\item \textsuperscript{145} Article 15 of the GDPR; article 14 of the LED.
\item \textsuperscript{146} Article 23 of the GDPR; article 15 of the LED.
\item \textsuperscript{147} Recital 46 of the AMLD4.
\end{itemize}
rules require. The AML Directives therefore seem compliant with the GDPR and the LED in this regard.

The obligation to notify a data subject about the processing should be especially important in relation to the bank register. Since it is easy for authorities to get an overview of an individual’s life through the bank register, the data subjects can without a notification feel like they are under constant surveillance. At the same time, it seems motivated that the subject should not be notified if it can impede an investigation since that would make the processing pointless. Although the AML Directives seem to comply with the GDPR and the LED in this regard, this notification process could still be in conflict with the Charter, something that will be discussed in section 4.6.3.5.

3.3.1.2 Purpose Limitation

The purpose of processing information in the AML Directives must also follow the principle of purpose limitation. Purpose limitation means that the personal data shall be collected for a “specified, explicit and legitimate” purpose and not processed in a way that is incompatible with that purpose. The purpose has to be clear in order for the data subject to be able to foresee when and for what their data will be processed. Case law is important when determining if foreseeable has been met. The purpose of the AML Directives should be seen as a rather clear when it comes to the storing of the data, as it is stored there to be easily accessible for authorities in order to fight crime. If it is necessary to be stored in this manner to fulfil that purpose is another question that will be discussed in the following section 3.3.1.3.

The initial retention of personal data in the bank register seems to be for the AML purpose. However, the subsequent access could be more problematic. When FIUs access the bank register, the purpose also seems rather clear since this authority is created for AML purposes. Considering that they look different in different MS though, they might still serve slightly different purposes, e.g. law enforcement, administration, or both. Since the GDPR and the LED differ they have in some way considered these

---

148 Article 79 of the GDPR; article 54 of the LED; recital 46 of the AMLD4.
149 Article 5.1.b of the GDPR; article 4.1.b of the LED.
150 Recital 41 of the GDPR; recital 33 of the LED.
151 Recital 41 of the GDPR; recital 33 of the LED.
152 Article 32.1 of the AMLD4.
differences, but the AML Directives do not make any difference between different FIUs or other competent authorities.

Many different authorities can constitute competent authorities, but particularly tax authorities have gained importance. Since it is not regulated in more detail to what degree tax authorities can fulfil the purpose of AML prevention, it becomes unclear to what degree these authorities should be able to access the personal data for this purpose. Is for example the prevention of predicate offences also part of preventing money laundering? Although the different authorities are using the data for the same purpose, it is also likely that they would have different assessments of what is proportionate to the purpose.\textsuperscript{154}

As previously discussed in section 2.3.2, some new measures in AMLD5 indicate that tax evasion is becoming a policy goal in itself. This is based on, for example, that tax authorities now have a lot more access to information collected for AML purposes.\textsuperscript{155} The bank register is important in this context as it can give tax authorities a direct access to detailed information about individuals, which could be useful to fight tax evasion. As this purpose is only indicated and not explicit, the possibility exists that the data will be processed for a purpose that is not in accordance with the principle of purpose limitation.

Subsequent access to the data stored in the bank register, can be processed on a separate legal ground, but also on the ground that it is compatible with the initial processing.\textsuperscript{156} The GDPR and the LED differ when they further define how it should be determined if the purpose of the subsequent processing is compatible with the initial one. In the GDPR, there is a list of factors that should be considered, such as the link between the purposes, the context the data has been collected in and possible consequences of the processing.\textsuperscript{157} In the LED, the provision is not as precise regarding the criteria but only states that the purpose is compatible, if the controller is authorised to process such data and if it is necessary and proportionate to fulfil the other purpose.\textsuperscript{158} The authorities seem to have more discretion to determine if the processing is compatible or not according to the LED than to the GDPR. This could be necessary in law enforcement as more flexibility could be required in order to investigate crimes efficiently. This discrepancy can affect the sharing between different FIUs as they would exchange information in accordance to different standards.

\textsuperscript{154} EDPS Opinion 1/2017, para 31.
\textsuperscript{155} EDPS Opinion 1/2017, para 18.
\textsuperscript{156} Article 5.1.b of the GDPR; article 4.1.b of the LED.
\textsuperscript{157} Article 6.4 of the GDPR.
\textsuperscript{158} Article 4.2 of the LED.
Access by for example tax authorities to defeat a predicate offence can, thus, also be legal on the ground that it is compatible with the initial AML purpose. Such an assessment can be done in accordance with the data protection laws, but the AML Directives does not give any guidance on how such an assessment would be or the limits for such an interpretation. One possible scenario is that the competent authorities make an assessment that e.g. defeating tax evasion is compatible. There seems to be nothing in the AML Directives that would hinder such an interpretation. It seems as if both the initial purpose and compatibility criterion are unclear and therefore it is hard to foresee what purpose motivates the processing of the data.

The sharing of information across boarders can also make the purpose of the processing unclear. Since the compatibility might be assessed in accordance with the GDPR in some MS and with the LED in other MS, what is considered compatible might differ.\(^\text{159}\) Since it is not clear in the AML Directives what constitutes a compatible purpose this will not help to harmonise the divergence between the MS. Tax crimes can also be mentioned here since they can be defined differently in different MS and yet that should not hinder the exchange of information.\(^\text{160}\) Different MS might therefore have different views of the seriousness of tax crimes, as well as if and when information shall be shared for such purposes.

The problem with the AML Directives in relation to purpose limitations is that the purposes are not specific enough. This can also affect the proportionality assessment in relation to the principle of data minimisation. This will be discussed in the following section.

3.3.1.3 Data Minimisation

The processing of personal data must also be necessary in order to achieve the purpose, in this case the public interest.\(^\text{161}\) The processing is necessary, only if the purpose could not be fulfilled by other means.\(^\text{162}\) This principle is referred to as data minimisation. In relation to data minimisation is also the storage limitation principle, which will be discussed in section 3.3.1.5.\(^\text{163}\) The principle of data minimisation differs in the GDPR

---

159 Quintel, *Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules*, p 46.
160 Article 1.36 of the AMLD5.
161 Article 5.1.c of the GDPR.
162 Recital 39 of the GDPR.
163 Recital 39 of the GDPR; recital 26 of the LED.
and the LED. Instead of a criterion that the processing needs to be *necessary* in relation to the purpose for which it is processed, the LED requires that the processing is *not excessive* in relation to the purpose.\textsuperscript{164} The threshold for what is necessary is therefore lower for processing in the LED than the GDPR.

The type of information that is stored in the bank register ought, in accordance with the principle of data minimisation, to be limited to what is necessary or not excessive. As mentioned, the purpose for introducing the bank register was to make the process of detecting and investigating crimes. The storing of information should therefore be proportional to achieve this. The information required to be stored in the bank register, e.g. IBAN and personal identification number, seems to be well motivated as it allows for an overview. As stated, the MS can also include other data in the bank register that they deem *essential*. The criterion of essential in the AML Directives seems to be higher the criteria of necessary and not excessive in the GDPR and the LED, why it does not seem to be a conflict. The AML Directives do not specify what should be considered essential or how that assessment shall be conducted, which will be further discussed in relation to the Charter, particularly in section 4.6.2.2.

The access of the FIUs and competent authorities should also be limited to what is necessary. The FIUs have immediate and unfiltered access, whilst the competent authorities have access to the extent they need to fulfil their obligations under the AML Directives.\textsuperscript{165} This shows on a particularly broad access for FIUs. If this is proportional is hard to determine as the proportionality assessment is affected by the fact that the purpose is already unclear. That the access to information in the bank register is based on a need-to-know basis indicates that there should be some sort of proportionality test, but the AML Directives do not specify what facts should be regarded in the context of AML.\textsuperscript{166} Since some measures might be proportional to fight terrorism and not to fight tax crimes, if both of these are to be purposes of the AML Directives, the legislator should be clearer of what is necessary or not excessive in relation to the different purposes.\textsuperscript{167}

This section has identified some problems with the assessment of proportionality. In relation to the Charter, the CJEU has set up more specific rules of what should be expected in the proportionality test, something that will discussed in the section 4.6.

\textsuperscript{164} Recital 26 & article 4.1.c of the LED.
\textsuperscript{165} Article 1.19 of the AMLD5.
\textsuperscript{166} Recital 21 of the AMLD5.
\textsuperscript{167} EDPS Opinion 1/2017, paras 25, 26 & 66.
3.3.1.4 Accuracy

The principle of accuracy means that the personal data should be kept up to date and inaccurate data should be erased or rectified.\textsuperscript{168} The processing could also be restricted if the accuracy of the data is contested by the data subject.\textsuperscript{169} There does not seem to be any rules in the AML Directives that would be in conflict with this obligation in the data protection laws. To carry out efficient investigations, it is also of importance that the information in the bank register is up to date and accurate.

3.3.1.5 Storage Limitation

Both the GDPR and the LED codify the storage limitation principle.\textsuperscript{170} This part of the right to erasure means that the personal data must be deleted or anonymised when it is no longer necessary for the purpose it is collected for.\textsuperscript{171} The controller should establish time limits for periodic review and erasure according to both the GDPR and the LED.\textsuperscript{172} As stated, such a time limit of five years is required for the processing of information in the bank register. There is also a possibility for extension for an additional five years.

The AML Directives do not state any criteria of what should be considered as necessary for the extension. As the AML Directives state that the extension should not be done on a case-by-case basis, it seems as if the extension can be general and does not need to consider what is necessary in each separate case.\textsuperscript{173} Although the other rules concerning retention is the same for the initial collection of the data by the obliged entities, the instruction to extend the retention period on a general basis is only in relation to the bank register.

This instruction could be a possible clash between the AML Directives and the data protection laws as the latter require that the information is kept for no longer than what is necessary. If there is no assessment of this necessary criterion in each case, it would not be possible to know if the extension actually is necessary in that case. It would then be the same as not having any assessment at all. What also indicates a conflict in this case, is that the initial retention period of five years was chosen due to data protection concerns.

\textsuperscript{168} Article 5.1.d of the GDPR; article 4.1.d of the LED.
\textsuperscript{169} Article 18.1.a of the GDPR; article 16.3.a of the LED.
\textsuperscript{170} Article 5.1.e of the GDPR; article 4.1.e of the LED.
\textsuperscript{171} Article 17.1.a of the GDPR; articles 4.1.e & 16 of the LED.
\textsuperscript{172} Recital 39 of the GDPR; recital 26 & article 5 of the LED.
\textsuperscript{173} Recital 21 of the AMLD5.
This indicates that the legislator thought that a set time of five years should be the rule for what is to be considered as necessary for data protection. It seems contrary therefore to encourage a general extension of this period, as that then would become the main rule for the information in the bank register.

Since the general basis for extension of the retention period shall be provided for in law, it could be argued that the legal provision would have considered what is necessary in different situations.\textsuperscript{174} However, the AML Directives do not seem to require that the law should consider what is necessary, but simply can state that the retention period should be extended in general.

According to LED, information may sometimes be restricted rather than erased, for example when the personal data must be maintained for the purpose of evidence.\textsuperscript{175} This rule does not have an equivalent in the GDPR and shows how the LED has taken into consideration the special character of law enforcement. The provision could allow for a greater possibility for the retention period to be prolonged, although the AML Directives do not state that any restriction in relation to the extended period is possible. The AML Directives, do however, not seemingly hinder that some of the information in the register was stored for longer time than other, which would be a restriction. This provision does not have any significance though, if there already is a possibility to prolong the retention period at a general basis without the fulfilling the criteria of this provision in the LED.

On this background, it seems as if the set-up of the retention period in the bank register can be in a potential conflict with the principle of storage limitation in the GDPR and the LED.

3.3.1.6 Integrity and Confidentiality

The principle of integrity and confidentiality is also codified in the data protection law.\textsuperscript{176} When implementing such measures, the controller shall take certain aspects into account, like the nature of the data and different risks.\textsuperscript{177} Although the security measures that have to be implemented somewhat differ, there is no significant difference between the GDPR and the LED in this regard. The MS should, according to both frameworks, ensure an appropriate level of risk, taking into consideration the state of the art, the cost, the nature,
scope, context and purpose of the processing as well as the risk of likelihood and severity for the rights and freedoms of natural persons. In the LED it is added that the level of security cannot depend on economic considerations alone.

As described in section 2.4.2, there are some security measures specified in the AML Directives, such as confidentiality measures and that other security measures for the data should be laid down. These measures are not further specified, but as the AML Directives also shall comply with the data protection laws, the MS must follow the criteria in the GDPR and the LED when they introduce the bank register. At this stage, it therefore does not seem to be any conflict between provisions in the data protection law and provisions the AML Directives, in relation to this. Most likely this is because the AML Directives do not lay down precise criteria that could go against data protection law. Instead the data protection laws complement the AML Directives. This balance that the legislator has chosen, could however be problematic in relation to the Charter, which will be discussed in section 4.6.

3.4 Summary

A couple of potential problems between the bank register and the GDPR and the LED have been identified in this section. One of them is the unclarity of the extension of the retention period that is not clearly defined. Another is the unclarity of the purpose of some of the processing that also affects the assessment of whether the processing in a particular situation is proportional. In addition, there is some uncertainty relating to who the controller is, which can make it difficult to determine who shall be held accountable for compliance with data protection law. The principles of lawfulness, fairness and transparency as well as integrity and confidentiality do not appear problematic on this level. The following section will discuss if the AML Directives, together with the safeguards in the GDPR and the LED, is in potential conflict with articles 7 and 8 of the Charter, which also indirectly affects the relationship between the GDPR, the LED and the Charter.

178 Recitals 83–84 & article 32 of the GDPR; recitals 28 & 60 & article 29 of the LED.
179 Recital 53 of the LED.
The Right to Protection of Personal Data and Private Life in the Charter

4.1 Introduction

As a part of EU primary law, the rights in the Charter shall guide all application of EU law, including the AML Directives, the GDPR and the LED. It is also stated in these frameworks that the Charter should be respected. The Charter provide a right for respect for private life in article 7. In parallel to this provision the Charter also establishes a right to protection of personal data in article 8. There is no case law regarding these provisions and the bank register, since the requirement to put in place such a register is new. There is, however, other case law from the CJEU that could be used as an analogy.

The cases that primarily will be analysed are Digital Rights Ireland and Tele2 Sverige AB. These cases concern the retention of personal data for the purpose of preventing serious crime, such as terrorism, through means of telecommunication. Many of the circumstances in these cases are similar to those in the bank register, why they are suitable as guidance. It is also argued in doctrine that these cases could apply to other types of data which still can be used to draw precise conclusions the private lives of many individuals. This is because the CJEU relies heavily on the Charter which indicates that this is an interpretation of those provisions. As the CJEU seems to be strengthening the protection of articles 7 and 8 of the Charter, it is also likely that they would make a strict interpretation in relation to the bank register. As concluded in section 2.4.1, such conclusions could be possible to draw from the information in the bank register. When the data in the register does not allow for as precise conclusions, these cases could, however, be less relevant. In these cases, the CJEU also provide

---

180 Recital 65 of the AMLD; recital 51 of the AMLD5; recital 4 of the GDPR; recital 46 of the LED.
181 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication, judgment 8 April 2014, (Digital Rights Ireland).
183 Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 170.
184 Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 170.
detailed criteria for when legislation, on both national and EU level, that require storing and sharing personal data can be considered lawful.

This section will begin by providing a background for the cases and then continue with an analysis of the potential conflicts between the data protection for information in the bank register and the Charter with these cases as guidance.

4.2 Digital Rights Ireland and Tele2 Sverige AB

*Digital Rights Ireland* concerned the validity of Directive 2006/24/EC\(^{186}\) that required providers of public communication networks to retain telecommunication data for all their users for the purpose of fighting crime, under a period from six months up to two years.\(^{187}\) The data that was retained constituted of personal data that could identify the individual, time and place of communication and what type of communication it was.\(^{188}\) What was said in the communication was not retained. The CJEU concluded that it was an extensive interference with articles 7 and 8 of the Charter, especially since the data subject was not informed when their data was accessed and could therefore feel like they were under constant surveillance.\(^{189}\) Interferences with the protection of private life have to be limited to what is strictly necessary.\(^{190}\) The interference was not considered strictly necessary in this case, mainly because there were no specific safeguards, both in the form of technical and organisational measures as well as limits of the processing of the data.\(^{191}\)

In relation to this, it was to be noted that the Directive was so general that the interference affected basically the entire European population.\(^{192}\) The Directive was against this background annulled.\(^{193}\) After the invalidation of Directive 2006/24/EC, many questions were raised in relation to national surveillance laws. This resulted in a case before the CJEU called *Tele2 Sverige AB*.

---

\(^{186}\) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

\(^{187}\) *Digital Rights Ireland*, para 23; articles 1, 5 & 6 of Directive 2006/24/EC.

\(^{188}\) *Digital Rights Ireland*, para 26.

\(^{189}\) *Digital Rights Ireland*, para 37.

\(^{190}\) *Digital Rights Ireland*, para 52.

\(^{191}\) *Digital Rights Ireland*, paras 66–67.

\(^{192}\) *Digital Rights Ireland*, para 56.

\(^{193}\) *Digital Rights Ireland*, paras 69 & 71.
After the invalidation of Directive 2006/24/EC, Directive 2002/58/EC\textsuperscript{194} applied to ensure that the right to privacy in the Charter was respected. This Directive included a provision that allowed for restrictions on the rights of data subjects for crime prevention.\textsuperscript{195} The question brought up in this case was whether the national legislation to retain traffic data in a general manner was compatible with the Directive in the light of the provisions in the Charter, after the annulment of Directive 2006/24/EC.\textsuperscript{196}

The data that was subject to retention in this case was in essence the same as the data in \textit{Digital Rights Ireland}.\textsuperscript{197} Also in \textit{Tele2 Sverige AB} could the interference only be justified to the extent that it was strictly necessary.\textsuperscript{198} In this case, the CJEU made a difference between the retention of the data and the sharing of it in the form of access by authorities. Regarding the retention, the CJEU concluded that the national laws could not be regarded as limited to what was strictly necessary, as they provided for “\textit{general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication}”.\textsuperscript{199} More specifically, the legislation had to be more precise about the situations that the data retention measures would be acceptable and also provide objective criteria of what could be a link between an individual and the fight against serious crimes based on objective evidence.\textsuperscript{200}

Regarding the access, the CJEU found that the legislation had to clearly lay down conditions that governed the access for authorities.\textsuperscript{201} These conditions should require that the access is restricted to the sole purpose of fighting serious crime, require that the access is subject to prior review by a court or independent administrative authority and that it is retained within the EU.\textsuperscript{202} The criteria that the CJEU has set out in these two cases will guide the remaining analysis in this section.

\textsuperscript{194} Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
\textsuperscript{195} \textit{Tele2 Sverige AB}, para 11; article 15 of Directive 2002/58/EC.
\textsuperscript{196} \textit{Tele2 Sverige AB}, paras 51 & 59.
\textsuperscript{197} \textit{Tele2 Sverige AB}, para 97.
\textsuperscript{198} \textit{Tele2 Sverige AB}, para 96; \textit{Digital Rights Ireland}, para 52.
\textsuperscript{199} \textit{Tele2 Sverige AB}, para 112.
\textsuperscript{200} \textit{Tele2 Sverige AB}, paras 109–111.
\textsuperscript{201} \textit{Tele2 Sverige AB}, para 118; \textit{Digital Rights Ireland}, para 61.
\textsuperscript{202} \textit{Tele2 Sverige AB}, para 125.
4.3 Application

As stated, this analysis concern articles 7 and 8 of the Charter. Article 8 of the Charter applies to personal data, which has already been defined in relation to the GDPR and the LED in section 3.2. It can therefore be concluded that article 8 of the Charter will apply to the bank register.

The protection of personal data in article 8 of the Charter is of fundamental importance to the protection of private life in article 7 of the Charter. Article 7 of the Charter only protect personal data that relates to private or family life. The definition of private life in article 7 of the Charter, should be broad like the definition of private life in article 8 of the ECHR. If particular information relates to private life or not is determined by the context, nature of the records, and how it is processed and obtained. The ECtHR has ruled that bank documents, collected for an investigation on among other things, money laundering, undoubtedly constitute personal data that relates to private life, whether or not the information is sensitive. The banking documents in that case consisted of transaction records, cheques, fiduciary dispositions and emails. The bank register in AMLD5 is not required to hold all of this information, but it is possible that it could, why considering its broad definition, article 7 of the Charter would probably apply to most of the personal data in the bank register.

The information required to be contained in the bank register, e.g. the IBAN, identification number and name, would probably fall into the scope of article 7 of the bank register as well. First of all, this bank information is not something that many people would give away lightly. The bank information is also usually under confidentiality, for example because it can be used to hurt an individual, for example by being used for fraud or even to use the payment account for money laundering. It can also be mentioned that this information can lead the authorities to all places where they can find the more detailed information about a person’s life, for example bank statements. Finally, it is also possible to draw conclusions of relations between different people and their business engagements.

203 ECtHR, S. and Marper v. the United Kingdom, judgment of 16 February 2000, para 103.
205 Schek, para 59; Amann v. Switzerland, para 65.
206 S. and Marper v. the United Kingdom, para 67.
207 Digital Rights Ireland, para 33; Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, judgment of 20 May 2003, para 75; ECtHR, M.N. and Others v. San Marino, judgment of 7 July 2015, para 51.
such as shareholding in a company. These things should definitely be considered to fall within the sphere of private life.\textsuperscript{209} It is therefore likely that also the most basic information in the bank register would fall within the scope of articles 7 and 8 of the Charter.

4.4 Interference

The mere storing of information by a public authority related to private life constitutes an interference, as well as the sharing of such data.\textsuperscript{210} Therefore the storing of personal data in the form of a bank register can constitute an interference in itself. The subsequent access by public authorities to the information will constitute another interference.

The degree of seriousness of the interference can also be of importance to the analysis. \textit{Tele2 Sverige AB} established that some interferences that are considered serious, only can be justified with the objective to fight serious crime.\textsuperscript{211} A serious interference can also mean that the legislator has less discretion.\textsuperscript{212}

Stored data that allow for very precise conclusions of a person’s private life to be drawn, e.g. habits of everyday life, activities carried out and the social relationships of individuals, are considered serious breaches.\textsuperscript{213} The CJEU also brought up that the data subjects might feel like they are under constant surveillance as they would not be informed when the information is accessed, which also could make the interference serious.\textsuperscript{214}

In \textit{Tele2 Sverige AB}, the personal data that was stored also could allow for a picture of a person’s life that was as sensitive as the actual content of the communication.\textsuperscript{215} If the bank statements of the accounts were accessible through the bank register it could be easy to get an extensive view of a person’s life. Most people today use a payment account to store their money and make the majority of their purchases with a card or other electronic mean that is connected to this account. It would therefore be easy to draw

\textsuperscript{209} Amann v. Switzerland, para 65; Scheke, para 59.
\textsuperscript{210} Amann v. Switzerland, para 69; Leander v. Sweden, para 48.
\textsuperscript{211} Tele2 Sverige AB, para 115.
\textsuperscript{212} Digital Rights Ireland, para 47; S and Marper v. the UK, para 102.
\textsuperscript{213} Tele2 Sverige AB, paras 99–100; Digital Rights Ireland, paras 27 & 37.
\textsuperscript{214} Tele2 Sverige AB, para 100; Digital Rights Ireland, para 37.
conclusions about a person’s life and everyday habits, activities carried out and their
social relationships. Just like in Tele2 Sverige AB and Digital Rights Ireland, the
interference would then be considered serious.\footnote{Tele2 Sverige AB, paras 99–100; Digital Rights Ireland, paras 27 & 37.} In a recent report from the European
Commission about the implementation of the bank registers, there are a few MS that have
reported that they might include information about transactions.\footnote{Report on the interconnection of national centralized automated mechanism (central registries or central
electronic data retrieval systems) of the Member States on bank accounts, COM (2019) 372 final, p 2, footnote 9.}

The bank statements are not required to be held in the bank register, but only the
information mentioned in section 2.4.1, e.g. IBAN and personal identification number.\footnote{Article 1.19 of the AMLD5.} This kind of information could not in the same way give an overview of a person’s
everyday life, although one can draw some conclusions e.g. about private and business relations. That information alone would, would therefore, probably not constitute a
serious interference. A serious interference cannot, however, be excluded because of the
possibility to include additional information.

It should be mentioned though that there is a significant difference with retaining
personal data in a bank register with all the information at one place, then at each separate
entity that has collected it. In the cases regarding telecommunication, it was the
telecommunication companies that retained the personal data, the authorities therefore
had to access the data for each one of them. This is the case with the bank information
outside the bank register, but with the bank register all the information will instead be
stored at the same place and accessible at the same time. This will make it easier for the
person who accesses the information to get an overview over the person’s financial
engagements. In the next step, they will be able to request information that can be detailed
regarding all entities this individual has relations with. The bank register will therefore
be a good tool to get a more extensive overview of a person’s life which should affect the
degree of the interference.

As brought up in section 3.3.1.1, data subjects likely would not be notified right
away when the information about them in the bank register is accessed. Due to the
purpose of the bank register, it is likely that the processing in many cases could impede
an investigation and thus an early notification of processing ought to be the exception
rather than the rule. Individuals would therefore feel like they are under constant
surveillance, like the data subjects in the telecommunication cases. It will not be possible
for the data subjects to escape this surveillance by using a smaller obliged entity that the authorities probably will not request information from, like it was before the bank register. This is one of the reasons for introducing the bank register, which is understandable, but at the same time it could speak for the processing being a particularly serious interference.

Furthermore, considering that the AML Directives does not specify what data can be included in the Directive or is laying down any specific criteria for what is essential, a serious breach cannot be excluded. Since essential is an even stricter criterion for data minimisation that the ones for data minimisation in the GDPR and the LED, those frameworks would not contribute to a better protection. Therefore, the AML Directives could possibly entail a serious interference of articles 7 and 8 of the Charter. Whether or not the interference is serious could of course affect the assessment under all the following points, but since a serious interference cannot be excluded the cases are relevant.

4.5 Lawful Limitations: Legal Basis, Essence of the Right and Objective of General Interest

Whether it is a serious interference or not, the interference can be limited in accordance with article 52.1 of the Charter. The conditions for such a limitation is: that it has to be provided for in law, respect the essence of the right, meet an objective of general interest and be proportional.\(^\text{219}\) To be proportional the measure has to be appropriate and necessary.\(^\text{220}\) An interference with articles 7 and 8 of the Charter can only be justified to the extent that it is strictly necessary.\(^\text{221}\) In this section, it will first be assessed if both the storing and sharing of the personal data in the bank register fulfils the first three criteria. In the subsequent section, it will then be assessed whether the storing and access fulfil the principle of proportionality.

It is rather clear in this case that there is a legal basis for the limitation as the bank register is part of AMLD4 and AMLD5, which have been passed following the relevant provisions in primary law. The AML Directives have also been published and are therefore accessible. The quality of the law also have to be sufficient in order for it to be foreseeable.\(^\text{222}\) How clear and precise the law is determines its quality, and the threshold

\(^{219}\) Article 52.1 of the Charter.  
\(^{220}\) Digital Rights Ireland, para 46; Scheke, para 74.  
\(^{221}\) Tele2 Sverige AB, para 96; Digital Rights Ireland, para 52.  
\(^{222}\) ECtHR, Silver and Others v. the United Kingdom, judgment of 25 March 1983, para 88.
depends on the seriousness of the interference.\textsuperscript{223} The quality of the law can be discussed in relation to the bank register, but in the cases that will be used for the analysis, this is discussed in relation to the proportionality assessment, why this thesis also will follow this structure.

The limit must also respect the essence of the right. In the telecommunication cases, the essence was not compromised; first, because the content of the conversations was not directly accessible and, secondly, because the Directive required some principles of data protection to be followed.\textsuperscript{224} The CJEU does not motivate this conclusion further. This could seem a bit strange considering that the CJEU also acknowledges the Advocate General’s conclusion that the information can be as useful to establish a profile of an individual as the content of the conversations.\textsuperscript{225} At the same time, it seems to be a reasonable conclusion that listening to an individual’s phone calls would be a more serious interference with privacy than storing information about the time and place of it, although that information was as useful in this particular case.

The bank register will probably respect the essence of the rights. If one would compare the content in telecommunication with the content in the bank register, which reasonably could be the bank statements, it seems as if the content of a phone call would be a more sensitive. Even if bank statements would be included in the bank register, it would therefore probably still be considered to respect the essence of the right. Furthermore, the AML Directives also ensures some data protection, for example technical measures to ensure no accidental loss, alteration or unlawful destruction.\textsuperscript{226} If these safeguards suffice will be discussed further in relation to proportionality. They should, however, be enough to respect the essence of the right.

Lastly, the limit must meet an objective of general interest within the EU. In Digital Rights Ireland the fight against terrorism was an objective of general interest. Prevention of crime, in a case with money laundering, has also been considered a legitimate aim for derogating article 8 of the ECHR.\textsuperscript{227} It is therefore likely that the AML Directives meet an objective of general interest.

\textsuperscript{223} Case C-355/10, European Parliament vs Council of the European Union, judgment of 5 September 2012, para 77.
\textsuperscript{224} Tele2 Sverige AB, para 101; Digital Rights Ireland, paras 28 & 39–40.
\textsuperscript{225} Tele2 Sverige AB, para 99; Opinion of the Advocate General Saugmandsgaard Øe, Tele2 Sverige AB, paras 253–254 & 257–259.
\textsuperscript{226} Recital 39 & article 5.1.f of the GDPR; recital 28 & article 4.1.f. of the LED.
\textsuperscript{227} M.N. and Others v. San Marino, para 75.
As these three criteria most likely would be fulfilled, it will be relevant to analyse if the bank register makes for a proportional interference.

### 4.6 Proportionality

#### 4.6.1 Appropriate

The final criteria for a lawful limitation is the proportionality test.\textsuperscript{228} The first part of the test is appropriateness, which means that the measure must have a connection with the purpose.\textsuperscript{229} In *Digital Rights Ireland*, the measure was seen as appropriate since it was a valuable tool for criminal investigations of terrorism, essentially because of the growing importance of electronic communications.\textsuperscript{230} Using payment accounts and electronic payment is also of growing importance in modern society, not the least for money laundering. The benefits that were brought up in section 2.4.2, like the possibility for fast access to get a complete picture of an individual’s economic engagement, speaks for the bank register being a valuable tool for AML. The bank register would therefore likely be considered appropriate for this aim.

The second part of the test is to determine if the interference is limited to what is strictly necessary.\textsuperscript{231} This could differ between the storing and sharing of the personal data in the bank register. In the following two sections, the thesis will discuss how the storing and sharing of information in the bank register relate to the criteria for what is strictly necessary according to CJEU case law. It is important to remember that the proportionality assessment also shall be strict when the interference can be regarded as serious which it can be in this case.\textsuperscript{232}

#### 4.6.2 Is the Storing of Personal Data in the Bank Register Strictly Necessary?

##### 4.6.2.1 Introduction

*Tele2 Sverige AB* made clear that storing, or retaining, personal data for the purpose of preventing serious crime is not unlawful, as long as it is limited to what is *strictly*

\textsuperscript{228} Article 52.1 of the Charter.
\textsuperscript{229} *Digital Rights Ireland*, para 46; *Scheke*, para 74.
\textsuperscript{230} *Digital Rights Ireland*, para 49.
\textsuperscript{231} *Tele2 Sverige AB*, para 96; *Digital Rights Ireland*, para 52; *Scheke*, para 77.
\textsuperscript{232} *Digital Rights Ireland*, paras 47 & 48; *S. and Marper v. United Kingdom*, para 102.
necessary.\textsuperscript{233} Such legislation cannot be considered strictly necessary if it provides for general and indiscriminate retention of all data, for all subscribers and all means of communication.\textsuperscript{234}

The main problem with the required retention in the telecommunication cases seemed to be that it had become the rule and not the exception as it affected everyone, even those with no link to a serious criminal offence.\textsuperscript{235} The link should be based on “(i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime”.\textsuperscript{236} These objective criteria for establishing a link may vary depending on the nature of the measure taken, but there should nevertheless be some objective criteria to establish a link between the data subject and the crime, which in practice limits the retention.\textsuperscript{237}

In addition, the legislation shall impose minimum safeguards to protect the personal data from misuse.\textsuperscript{238} The retention period also had to be limited to what is strictly necessary and the data must be irreversibly destroyed at the end of the retention period.\textsuperscript{239} All rules that govern the scope of the data retention measures should according to the CJEU be clear and precise.\textsuperscript{240} Furthermore, the CJEU states that storing and sharing data in this way only can be justified by the purpose of fighting serious crime.\textsuperscript{241} As stated in section 3.3.1.2 the storing of data in the bank register rather clearly seems to be for the purpose of AML. The subsequent access, however, could possibly be done for other purposes as well, why this criterion will be discussed in relation to access in section 4.6.3.

This section is divided into the criterion for establishing a link, the retention period and the security measures. An assessment if the rules are clear and precise will be done for each rule under each section.
4.6.2.2 Link Between Data Subject and Criminal Activity

When the CJEU determined if the legislation in Digital Rights Ireland was to be considered strictly necessary, it emphasised that the interference was far-reaching as it interfered with the rights of practically the entire European population, as everyone uses electric communication today.\textsuperscript{242} This showed that the Directive was general and that there was no link between the data subject and criminal activity. The same could be said in relation to the bank register. Since the majority of people today use some way of electronic payment connected to a payment account, the storing of information in the bank register would also affect basically the entire European population.

The CJEU states that the means of communication of the retained data shall be limited.\textsuperscript{243} In the context of the bank register, means of communication could probably translate to type of bank account. The one objective criterion that can be found in the Directive for the storing of information is that it should be a payment or bank account identified by IBAN.\textsuperscript{244} For the definition, AMLD5 refers to another regulation that defines payment account as an account used for transactions and IBAN as a number for a payment account as defined by the International Organisation for Standardisation (ISO).\textsuperscript{245} Including the IBAN could therefore indicate that only accounts possible to use for transferring money should be included in the register. If it is only these accounts that are listed in the bank register, the data will be limited in the sense that not all accounts of a data subject would be stored.

Since the objective criteria can depend on the nature of the measure, it is necessary to consider what this would mean in the context of the bank register. With that in consideration, it might not be much of a limitation to exclude some accounts as anyone who has an account of a different kind e.g. an investment account, would probably need a payment account to transfer money to and from that other account. Furthermore, it is not sufficient according to the judgment to only limit the data in one category to remove the general retention of the measure, why the bank register still could be problematic.\textsuperscript{246}

\textsuperscript{242}Digital Rights Ireland, para 56.
\textsuperscript{243}Tele2 Sverige AB, para 108.
\textsuperscript{244}1.19 of the AMLD5.
\textsuperscript{245}Articles 2.5 & 2.15 of Regulation (EU) No 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009.
\textsuperscript{246}Cameron, Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson, p 1486; Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 169.
Although the CJEU concludes that it is general to include the entire population of a country, it does not completely refute the possibility to use a geographical criterion to establish a link.²⁴⁷ The CJEU also mentions time period as a possible objective criterion. The bank register is not limited to any of these two criteria, and they would probably be hard to apply in relation to AML. Money laundering and terrorist financing are international crimes that should not be depended on any events in time.

The retention can also be limited to a group of persons likely to be involved according to the CJEU. That the bank register limits the data subjects to those with payment accounts, should be too broad to fulfil this criterion. It would be the same as including everyone who uses electric communication services, which the CJEU already refuted as a sufficient limitation.²⁴⁸ To limit the data subjects to a group of people in another way, should not be too challenging in the AML context though.

Many of the measures required according to the AML Directives are based on risk, e.g. the CDD measures. The risk-based approach would fit this third criterion well as the aim with the risk-based approach literally is to determine the risk with a certain customer. That the risk-based approach is more in line with proportionality and tends to result in sufficient data protection has also been argued by the EDPS.²⁴⁹ Although risk-assessments permeate the AML Directives, it does not appear in relation to the bank register. This shows on a shift that has occurred with AMLD5, which the bank register is part of, as discussed in section 2.4.1. The initial collection of information is still based on risk, and therefore obliged entities probably store more information on high-risk customers compared to customers with lower risk profiles. When the information is included in the bank register though, the amount of information can be the same for everyone. This might not seem significant in the relation to the information per se, as it is stored at the obliged entity anyway. However, it is the interference of keeping all this information at one place making it possible to get an overview over someone’s life that constitutes the serious interference. It is therefore reasonable that the bank register should be based on risk, or in some other way make a difference between individuals. That the risk-based approach is not used in the bank register is, thus, problematic.

The above shows that it does not appear to be any criterion in the AML Directives that establishes a link between the data subject and a serious crime and, thus, limit the

²⁴⁷ Tele2 Sverige AB, para 106; Digital Rights Ireland, para 59.
²⁴⁸ Tele2 Sverige AB, para 105, Digital Rights Ireland, paras 57–58.
retention. Instead the processing in the bank register affects all data subjects equally. Since the data is a bit different from the data in the telecommunication cases, the general character might be more acceptable in some cases in relation to the bank register. For example, if the bank register only contains the personal data that is required a general character might be acceptable, but if bank statements are included it most likely would not. This should be kept in mind when reading the analysis in the following sections.

The legislation should also lay down clear and precise rules governing the scope of the storing of data, in relation to the categories of data, means of communication, persons affected, and retention period adopted.\textsuperscript{250} This is probably in order for the limitation to be foreseeable and applied consistently. The bank register is specific about the data that is required to be in the register. However, the possibility for MS to also include information in the register that they find essential is not specified. As mentioned in section 3.3.1.3, the AML Directives do not specify what can or cannot be regarded as essential. As the GDPR and the LED only provide criteria that seems less strict than essential, namely necessary and not excessive, they do not work as safeguards in this case. In order to fulfil the criterion, it should at least be specified in the AML Directives what information is not to be considered limited to strictly necessary. In that way, the MS are given some discretion, but the measures are still limited in some way.

In conclusion, the bank register appears to be problematic in this regard as it does not specify what information cannot be included in the bank register or makes a sufficient delimitation in another way. That the bank register is limited to accounts with an IBAN and that only persons with payment accounts are affected, is too general to create a sufficient link between data subject and crime.

4.6.2.3 Retention Period

The CJEU does not set a specific time period in \textit{Tele2 Sverige AB} but states that the retention period has to be limited to what is strictly necessary.\textsuperscript{251} The legislation in this case did not specify a time period but only stated that the data should be retained for a limited time period.\textsuperscript{252} This resulted in various different retention periods in different MS.\textsuperscript{253} In the \textit{Digital Rights Ireland} case, the retention period of six months to two years

\textsuperscript{250} \textit{Tele2 Sverige AB}, paras 108–109; \textit{Digital Rights Ireland}, para 54.
\textsuperscript{251} \textit{Tele2 Sverige AB}, para 108.
\textsuperscript{252} \textit{Tele2 Sverige AB}, para 92.
\textsuperscript{253} Cameron, \textit{Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson}, p 1483.
was not proportional because the Directive did not state that the assessment of the exact retention period should be based on objective criteria that ensured that it was limited to what was strictly necessary.\textsuperscript{254} One interpretation of this criterion is that, since the retention period can have different lengths, the law have to lay down objective criteria that helps determine what length of the retention period is strictly necessary in a particular situation. For example, a longer retention period might be justified for some kind of data.

In contrast to the legislation in the telecommunication cases, the initial retention period in the bank register has been set to a specific time period of five years. There is neither any difference made between the retention period of different types of data or data subjects which indicates that the retention period is general. Although the retention period is set, it could fulfil this criterion, if the legislator can show that retention of all data in the register for five years is strictly necessary.

As stated in section 2.4.1, the reason behind the retention period of five years is data protection purposes and legal certainty as well as being able to effectively use it as evidence.\textsuperscript{255} This indicates that the legislator considered the time limit of five years to be a good balance between efficient investigations and respecting data protection rules. Such a balance could be understandable for some crimes such as terrorism financing and money laundering which can have been planned or carried out during a long period of time.\textsuperscript{256} The retention period was a lot shorter in the telecommunication cases, e.g. six months in the Swedish law in \textit{Tele2 Sverige AB} but for a similar reason.\textsuperscript{257} It should be considered though that the financing of a terrorist attack might be planned years before an attack and laundering money can be done years after a crime, or constantly over a time period. It therefore seems motivated with a five-year period, which then could be considered limited to what is strictly necessary for some serious crimes at least. For other crimes though, such as tax evasion, the time period might not be as suitable. As all data is retained to be available in case of more serious crimes, such as terrorist attacks, the retention period could be acceptable for the retention of all data. Whether or not the initial retention period can be considered strictly necessary, it is nevertheless defined and should therefore at least fulfil the CJEU’s requirement for being clear and precise.

\textsuperscript{254} Digital Rights Ireland, para 64.
\textsuperscript{255} Recital 44 of the AMLD4; article 4 of the Council Directive 91/308/EEC.
\textsuperscript{256} Cameron, \textit{Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson}, p 1483.
\textsuperscript{257} \textit{Tele2 Sverige AB}, para 19.
In section 3.3.1.5 it was concluded that the retention period could be in conflict with the GDPR and the LED when it comes to the extension that has been limited to what is necessary, but at the same time suggests that extension can be done on a general basis without case-by-case consideration. In relation to the Charter, this would probably be an issue since the extension is not as clear and precise as the case requires. It also cannot be ensured that the additional retention period is limited to what is considered strictly necessary, if the conditions for the extension are not defined. Furthermore, the limitation for the bank register is based on the criterion of necessary, whilst it is required according to the telecommunication cases that it should be limited to what is strictly necessary.

The initial retention period for the bank register could likely be considered strictly necessary. However, it is problematic that the criteria for an extension of the retention period are unclear.

4.6.2.4 Security Standards

The retention shall also be surrounded by safeguards to protect the personal data from misuse.\footnote{Tele2 Sverige AB, paras 108–109; Digital Rights Ireland, para 54.} There are two different kinds of risk for misuse that are relevant. One is the risk of abuse by the competent authorities, for example if they access more data than what is necessary. That will be discussed in section 4.6.3. Another risk, which will be discussed in this section, is that of unauthorised third-party access due to a lack of technical or organisational measures to protect the data. These two types of risks have also been identified in doctrine.\footnote{Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 169.} For the AML Directive to be strictly necessary, it has to impose minimum safeguards to ensure an effective protection against misuse according to the CJEU.\footnote{Tele2 Sverige AB, para 109; Digital Rights Ireland, para 54.}

The security level must correspond with the risks and potential consequences of a security breach. The CJEU makes the conclusion in the telecommunication cases that “the quantity and sensitivity of retained data, and the risk of unlawful access to it, require a particularly high level of protection and security”.\footnote{Tele2 Sverige AB, para 122; Digital Rights Ireland, paras 66–68.} This is also relevant in relation to the bank register. As discussed in section 4.3, bank information could be considered as sensitive as the data in the telecommunication cases, e.g. if they consist of bank
statements. This information could even be used for crimes such as fraud, black mail or even money laundering, which indicates a risk for unlawful access. In addition, the quantity of the information in the bank register should probably be considered especially high as all the information is stored in the same register and not spread out between several telecommunication companies. Unlawful access could then result in access to all data and not only a fraction of it.

As described in section 3.3.1.6, the security of the bank register is mainly regulated through the GDPR and the LED which both require the controller to take into account certain aspects like the nature of the data and different risks, when implementing security measures.\textsuperscript{262} The MS should in particular ensure an appropriate level of risk, taking into consideration e.g. the state of the art, the cost and the purpose of the processing.\textsuperscript{263} It is this balance that the legislator has chosen that now till be tried against the Charter.

One of the reasons the CJEU had for annulling Directive 2006/24/EC in \textit{Digital Rights Ireland} was that it allowed for cost to be a factor when setting the standard of the security measures, but did not balance this with other security measures.\textsuperscript{264} This has, however, changed with the GDPR and the LED which now provides several other objective factors, only one of them being the cost. This should mean that the balance between the cost and other security factors is more sufficient.

Furthermore, when the GDPR applies, the controller is also required to consult with the supervisory authority if the high risk cannot be mitigated with available technology and cost of implementation.\textsuperscript{265} This could also work as a safeguard to hinder the controller from overriding the risk based on the cost. In the LED, it is added that the level of security cannot depend on economic considerations alone, which also forbids such one-sided considerations.\textsuperscript{266} It would not be reasonable to eliminate cost as a factor to consider all together. The cost of retaining data was actually one of the reasons that Tele2 wanted to stop retaining data.\textsuperscript{267} Cost might be less of a problem in relation to the bank register though, since it will be administrated by the state, not commercial actors, and could result in lower costs considering improved efficiency as discussed in section 2.4.2.

\textsuperscript{262} Article 32 of the GDPR; article 29 of the LED.
\textsuperscript{263} Recitals 83-84 & article 32 of the GDPR; recitals 28 & 60 & article 29 of the LED.
\textsuperscript{264} Digital Rights Ireland, para 67, referring to article 7 of Directive 2006/24/EC, article 4.1 of Directive 2002/58/EC and article 17.1 of Directive 95/46/EC.
\textsuperscript{265} Recital 84 of the GDPR.
\textsuperscript{266} Recital 53 of the LED.
\textsuperscript{267} Cameron, Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson, p 1471.
Another security measure is to ensure that the data is destroyed at the end of the retention period.268 This is required for all the data in the bank register, unless it is necessary to extend the retention period.269 The Directive in Digital Rights Ireland included a provision of destruction for all data at the end of the retention period, except the data that have been accessed and preserved.270 This provision was not accepted by the CJEU.271 The bank register does not make any exception from the destruction of data at the end of the retention period, as it even requires the extension to be within a particular time period. This safeguard, as well as the other ones, does not seem to be problematic in relation to the bank register.

4.6.3 Is the Sharing of Personal Data in the Bank Register Strictly Necessary?

4.6.3.1 Introduction

The sharing of, or access to, personal data in the bank register constitutes an interference on its own as stated earlier. That interference must also be limited to what is strictly necessary.272 The sharing can only be justified by the objective to fight serious crime, like the storing.273 The legislation must also lay down clear and precise rules that specify under what circumstances access can be granted.274 It is not explicit enough to refer to the general purpose of the Directive to fight serious crime.275

To ensure that these rules are followed, the access should be subject to a prior review, unless in cases of urgency.276 In addition to this, there must be an independent authority that review the compliance with data protection rules.277 The data subject shall also be notified about the processing so that they have the possibility to seek judicial remedy, when there no longer is a risk to jeopardise the investigation.278 Like the storing,

---

268 Tele2 Sverige AB, para 122; Digital Rights Ireland, para 67.
269 Article 40.1 of the AMLD4.
270 Digital Rights Ireland, para 67, referring to article 7 of Directive 2006/24/EC.
271 Digital Rights Ireland, para 67, referring to article 7 of Directive 2006/24/EC.
272 Tele2 Sverige AB, para 116.
273 Tele2 Sverige AB, para 115.
274 Tele2 Sverige AB, para 117.
275 Tele2 Sverige AB, para 118; Digital Rights Ireland, para 61.
276 Tele2 Sverige AB, para 120.
277 Tele2 Sverige AB, para 123; Digital Rights Ireland, para 68; Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, judgment of 6 October 2015, (Schrems), paras 41 & 58.
278 Tele2 Sverige AB, para 121.
the sharing of data must be under sufficient safeguards to protect the data from misuse.\textsuperscript{279} To this relates that the data must be kept within the EU.\textsuperscript{280}

The following section is divided into the criterion for fighting serious crime, conditions for the access, prior review and supervision, and lastly, the safeguards, such as the requirement to retain the information within the EU. An assessment if the rules are clear and precise, will be done for each rule under each section

4.6.3.2 Objective to Fight Serious Crime

Only the objective of fighting serious crime could justify the access to retained data of the kind in the telecommunication cases.\textsuperscript{281} This can be a problem in relation to the bank register, since the data can be considered as sensitive, see section 4.3. Access to such information can then neither be justified by something other than fighting serious crime.

Serious crime is not clearly defined by the CJEU, but it gives organised crime and terrorism as examples.\textsuperscript{282} This indicates that only the most severe types of crime can legitimise this kind of processing.\textsuperscript{283} In doctrine, it is also argued that armed robbery and murder constitute serious crimes, which also has been the interpretation by the MS.\textsuperscript{284} The access to the bank register is clearly for the purposes of terrorist financing and money laundering of proceeds from organised crime. As discussed in section 3.3.1.2, there also seems to be other purposes in the AML Directives that the data could be shared for. One such possible policy purpose is tax evasion. Also, the EDPS brought up tax evasion as an emerging policy goal in its comment on the AMLD5 proposal.\textsuperscript{285} That tax authorities are supposed to have access to the bank register, which is the case in the adopted legislation even after the opinion by the EDPS, speaks for this conclusion.\textsuperscript{286} The question is if tax evasion can be considered a serious crime as defined by the CJEU in this case and also justify access to the data in the bank register. Otherwise, this measure would clearly not be strictly necessary for that purpose.

\begin{flushleft}
\textsuperscript{279} Tele2 Sverige AB, para 122; Digital Rights Ireland, paras 66–68.
\textsuperscript{280} Tele2 Sverige AB, para 122; Digital Rights Ireland, paras 66–68.
\textsuperscript{281} Tele2 Sverige AB, para 115; Digital Rights Ireland, para 60.
\textsuperscript{282} Tele2 Sverige AB, para 103; Digital Rights Ireland, para 51.
\textsuperscript{283} Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 168.
\textsuperscript{284} Cameron, Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson, p 1483.
\textsuperscript{285} EDPS Opinion 1/2017, para 26.
\textsuperscript{286} EDPS Opinion 1/2017, para 7.
\end{flushleft}
Tax evasion could range from more to less serious crimes. For example, the tax evasion could be part of a systematic or widespread operation that takes big sums of money from society. Such a scenario would probably be regarded as a serious crime as it is a form of organised crime that result in major damage on society. At the same time, it could most likely be used to finance other criminal activity. However, there are also less severe tax crimes that could be included. Tax crimes as defined in the AML Directives are predicate offences, only when they are punishable by deprivation of liberty for a minimum sentence of six months or a maximum sentence of one year. In Sweden for example, offences would be included that only has entailed a person to leave false information as that could lead to prison for up to two years. That this kind of tax evasion could be equal to the seriousness of terrorism financing and organised crime is unlikely.

Since the concept of serious crime is unclear, discretion to decide what constitutes a serious crime is given to the MS which can lead to different definition in different MS. As the MS particularly have different views of the severity of tax crimes, this could also lead to an uneven application within the EU. As the AML Directives provide for a limit of what tax crimes constitute predicate offences based on the length of the sentence, that hinders different applications to some extent. However, since the MS might have different definitions of tax crimes, heir view on the seriousness of the tax crime might differ, as well as what is considered strictly necessary to fight those crimes. One possible consequence is that for a tax crime with a prison sentence of two years can legitimise one way of access to the bank register in one MS, but not in another as the latter considers the crime to be less serious. This could also affect the cooperation between the MS as they would make the assessment according to different standards and might not want to share information for a crime that they do not regard as a serious crime, although the requesting MS does. This can affect the foreseeability of the rules.

This is problematic in relation to the bank register because that is a kind of storing and sharing that only can be justified by serious crime. Sharing information outside of the register might be justified by other purposes, which is outside the scope of this thesis to discuss. The purposes for which processing can be carried out has to be specified in order to fulfil the requirement of clarity of these rules is. That they are not clear, and that there

---

287 Article 3.4.f of the AMLD4.
288 Skattebrottslagen (1971:69) 2 §.
289 Cameron, Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson, p 1489; Møller Pedersen, Udsen & Sandfeld Jakobsen, Data retention in Europe—the Tele 2 Case and Beyond, p 168.
are several purposes will also affect the assessment of the rules for what is strictly necessary as purpose relates to the proportionality assessment. This will be discussed in the following section.

4.6.3.3 Conditions for the Access

The rules limiting the access to what is strictly necessary must also be clear and precise, like the rules regarding retention.\textsuperscript{290} What needs to be clear is under what circumstances and conditions the access to the data in the bank register can be granted.\textsuperscript{291} It should not be enough in this case to refer to the objective of the AML Directives, which is to prevent money laundering and terrorist financing.\textsuperscript{292} Instead, there should be objective criteria that determine the circumstances and conditions for the access.\textsuperscript{293} In relation to this, the CJEU lays down a general rule that for the objective of fighting crime, only data relating to individuals suspected to be involved in the crime can be accessed.\textsuperscript{294}

Even though the purpose is specified and only the serious crimes are to be included, they could also range from extremely severe, such as financing terrorist attacks, to less severe, such as organised system to launder money from tax evasion. What constitutes \textit{strictly necessary} might not to be the same in these cases. Since the rules regarding the access should be clear and precise it should be clear what is strictly necessary in relation to these different crimes in the bank register.

The bank register should be accessible in an \textit{“immediate and unfiltered manner to national FIUs”}.\textsuperscript{295} This does not indicate anything about the circumstances for which this access is allowed but only in which manner. As discussed in section 3.3.1.3, there is some indication of a proportionality test as the information still should be accessed on a need-to-know basis according to the recitals.\textsuperscript{296} The problem still remains that the legislation does not specify what should be considered in this assessment why the rules are not clear and precise.

Other competent authorities should also have access for \textit{“fulfilling their obligations under this Directive”}.\textsuperscript{297} Such a general reference to the purpose of the directive was not

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{290} Tele2 Sverige AB, para 117.
\item \textsuperscript{291} Tele2 Sverige AB, para 117.
\item \textsuperscript{292} Tele2 Sverige AB, para 118; Digital Rights Ireland, para 61.
\item \textsuperscript{293} Tele2 Sverige AB, para 119.
\item \textsuperscript{294} Tele2 Sverige AB, para 119; ECtHR, Zakharov v. Russia, judgment of 4 December 2015, para 260.
\item \textsuperscript{295} Article 1.19 of the AMLD5.
\item \textsuperscript{296} Recital 21 of the AMLD5.
\item \textsuperscript{297} Article 1.19 of the AMLD5.
\end{enumerate}
\end{footnotesize}
enough according to the CJEU.298 Access on a need-to-know basis also applies here but it is not further defined. Yet, clear and precise rules should be particularly important in relation to these authorities, as they serve many different purposes and would therefore likely access information according to different standards.

The LED and the GDPR do not provide any guidance for this limitation as they neither provide particular criteria that should be considered. Additionally, the access to the bank register must be limited to what is strictly necessary. The thresholds in the data protection laws though are not as strict as that of the CJEU, as the LED only demand that the access is *not excessive* when the GDPR states that it has to be *necessary*.

Since the criteria for the access to the information is unclear, it cannot be determined if the legislation follow the CJEU general rule that only data related to suspects should be accessed. Since that in itself is not laid down as a criterion, it is likely that the legislation regarding the bank register does comply with this general rule. The telecommunication cases also bring up an exception to the general rule that only data for suspects should be accessed. This exception is when there is an urgent security threat and access to the information could make a significant difference.299 Although, such an exception might occur in relation to the bank register, all access given to the FIUs or other competent authorities in the law, cannot be urgent. To be precise and clear this exception ought also to be specified in the legislation.

In order to ensure that an assessment for what is strictly necessary is conducted and correct, there should be safeguards. These requirements laid down by the CJEU, such as prior review and keeping the data within the EU will be discussed in the following sections.

4.6.3.4 Prior Review and Supervision

Although the law contains clear and precise criteria for the access, there is still a risk that the access can be abused through improper application of the criteria in practice. For that reason, the access to personal data should also be subject to a prior review by a court or an independent authority.300 A prior review can be particularly important when the data is subject to automatic processing and there is a significant risk of unlawful access to the

---

298 *Tele2 Sverige AB*, para 118; *Digital Rights Ireland*, para 61.
299 *Tele2 Sverige AB*, para 119.
300 *Tele2 Sverige AB*, para 120; *Digital Rights Ireland*, para 62.
The bank register is an automatic mechanism. There is also a high risk of unlawful abuse because of the way different authorities have access to the bank register.

It is argued in doctrine that intelligence authorities can constitute a higher risk of abuse than investigation authorities, as they base their access on relevance rather than need. This is because they tend to serve a broader function than conducting individual investigations of criminal cases. The FIUs in the bank register shall have access on a need-to-know basis as stated above. At the same time, the FIUs shall be able to access necessary information in the bank register without a prior report of suspicion having been filed. They should therefore not only conduct investigations, but can also access the basis on for example their own analysis. The EDPS pointed out that this broad access to information makes the FIUs take the form of intelligence agencies rather than investigation agencies. This suggests that there is a high risk of unlawful abuse of the access by FIUs. Yet, there is no prior review of access by FIUs as their access shall be direct, immediate and unfiltered.

The AML Directives do not seem to require a prior review of the access to information in the bank register by the other competent authorities neither, although the access of these authorises only should be for fulfilling their obligations under the AML Directives. It is not clear how these authorities have access, but they could possibly have direct access to some of the information in the bank register that is considered to be useful for their AML work. This does not mean though, that the information they technically have access to will always be strictly necessary to access in all cases. There is a high risk for abuse by these competent authorities in relation to the bank register as they do not only serve AML purposes but also other purposes, such as tax control, which the data in the bank register could be useful for. There is, however, an uncertainty whether these purposes constitute a serious crime as the case law requires, or even if it is a purpose that the AML Directives recognise as legitimate for the processing. Not having a prior

301 Digital Rights Ireland, para 55; S. and Marper v. United Kingdom, para 103.
302 Article 1.19 of the AMLD5.
305 Recital 17 & article 1.18 of the AMLD5
306 Recital 17 & article 1.18 of the AMLD5.
307 EDPS Opinion 1/2017, para 52.
308 Article 1.19 of the AMLD5.
309 Article 1.19 of the AMLD5.
review to ensure that the personal data is accessed only when strictly necessary is therefore especially problematic as the risk for abuse is high.

When sharing information with FIUs in other MS there is a kind of prior review by an independent authority as the FIU in the MS that receives the request, decide whether the personal data shall be shared or not.\textsuperscript{310} This might, however, not be sufficient as the FIUs might have an interest in a broad access themselves and therefore allow for a broad interpretation.\textsuperscript{311} Furthermore, it should also be mentioned in that there seems to be an aim to interconnect all the bank registers in the MS, which would mean that an FIU could access the bank register in another MS directly.\textsuperscript{312} As that would eliminate the prior review, this could become problematic in the future.

As there are no clear and precise conditions regarding the access, a prior review might not work as an effective safeguard though. As a prior review will only assess whether the criteria in the law are followed, it would probably accept access on criteria that are vague. The prior review would then not really serve its function to prevent abuse.\textsuperscript{313} It seems particularly necessary therefore, to first make sure that the criteria are sufficient and then put in place a prior review.

Exceptions from the prior review can be made in urgent cases. As argued in section 4.6.3.3, these cases cannot justify all access to the information in the bank register. A prior review would probably not even majorly affect the efficiency of the bank register. The efficiency argument that motivated the bank register was that it could give the authorities a quick overview so that they would know who they should turn to for more information. Although a prior review might postpone an overview slightly, the bank register would still make the procedure faster as the authorities would then know who to contact, and still do not have to turn to each financial actor separately. The benefits with the bank register will thus not be affected by a prior review.

In addition to the prior review, there must also be an independent authority that in general review the compliance with data protection rules.\textsuperscript{314} This relates to article 8.3 of the Charter that explicitly states this. For the bank register, this is regulated through the GDPR and the LED which state that the MS has to have a supervisory authority for this

\textsuperscript{310} Article 53 of the AMLD4; article 1.33 of the AMLD5.
\textsuperscript{311} Opinion of the Advocate General Saugmandsgaard Øe, \textit{Tele2 Sverige AB}, para 236.
\textsuperscript{312} Article 1.19 of the AMLD5.
\textsuperscript{313} Cameron, \textit{Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson}, p 1491.
\textsuperscript{314} \textit{Tele2 Sverige AB}, para 123; \textit{Digital Rights Ireland}, para 68; Schrems, paras 41 & 58.
These supervisory authorities shall be independent, which in line with the requirement of the CJEU. The bank register therefore seems to fulfil this requirement.

In conclusion, this section has shown that the criterion for a prior review can be problematic in relation to the bank register. A sufficient supervisory authority seems to be in place thought. In the next section, other safeguards that is required in case law will be discussed.

4.6.3.5 Other Safeguards

As stated in section 4.6.2.4, there is a risk for abuse both illegitimate third-party access and access by competent authorities. The access must be surrounded by safeguards to protect the personal data from both of these risks of misuse. In the bank register, it is stated that this should be done through secure channels and in a manner that ensures full confidentiality of enquiries according to AMLD4. The same rules in the GDPR and the LED that applied to the retention of data also applies here, namely that the MS shall take into consideration different aspects like the nature of the data and different risks, when implementing security measures. As concluded in section 4.6.2.4, these measures seem to be sufficient in relation to the bank register.

Sharing information through the bank register could actually also constitute a safeguard from third-party access by the design it has. Before the bank register, for example the FIUs had to turn to each obliged entity separately and ask for information about an individual, as described in section 2.4.2. Even the entities that do not have information about an individual, would then find out that there was a suspicion of money laundering related to this person. That could violate integrity as the entities would find out that an individual is being investigated, although it is later concluded that the individual was not involved in any crime. It is possible that the entity even would make a note about this for future reference, which can have consequences for this individual. With the bank register, the authorities do not have to request information from all actors, but instead use the bank register. They could, thereby, access information without telling the entities. In this way the bank register contributes to the strengthening of the privacy of an individual. It might not make up for the interference that the bank register constitutes

315 Article 51 of the GDPR; article 41 of the LED.
316 Article 52 of the GDPR; article 42 of the LED.
317 Tele2 Sverige AB, paras 108–109; Digital Rights Ireland, para 54.
318 Article 42 of the AMLD4.
in other ways, but it should be taken into consideration. To ensure safety from third-party access, the bank register could in this way be beneficial. The CJEU has though also laid down some other criteria to ensure protection from both third-party access and abuse by authorities which already have access.

The first of these criteria is that the data must be kept within the EU. According to the AML Directives, FIUs in the MS should exchange relevant information to FIUs in nations outside the EU, but only if it respects EU law. This means that the data only can be shared if it respects EU data protection laws including the Charter and, thus, this requirement in the case law. It would not matter if the GDPR and the LED allow for transfers of data to countries outside the EU, because the Charter will in this situation supersede them as it constitutes primary law. The bank register seems therefore to comply with the Charter in this regard.

Another mandatory criterion that the CJEU sets up is that the data subject must be notified about the processing, when such a notification could no longer harm the investigation, so that the data subjects could exercise their right to a legal remedy. Data protection law gives the data subjects a right to be notified if data is being processed in the bank register. This right can be restricted if that access can impede an ongoing investigation. There are also other exceptions, but they should not be applicable in this case. Otherwise, the processing authority must, thus, notify the data subject. Data subjects have a possibility to seek judicial remedy when they have been notified. In cases where it is unclear who the controller is, it can be problematic to find someone to hold accountable for compliance with these rules, just like it is in relation to the GDPR and the LED as discussed in section 3.2. Otherwise it seems as if the bank register fulfils this criterion of notification and the other criteria in this section.

319 *Tele2 Sverige AB*, para 122; *Digital Rights Ireland*, para 68.
320 Recital 58 of the AMLD4.
321 Articles 45–46 & 49 of the GDPR; articles 35–37 of the LED.
322 *Tele2 Sverige AB*, para 121.
323 Article 15 of the GDPR; article 14 of the LED; recital 46 of the AMLD4.
324 Article 23 of the GDPR; article 15 of the LED; recital 46 of the AMLD4.
325 Article 79 of the GDPR; article 54 of the LED; recital 46 of the AMLD4.
4.7 Summary

There seems to be some conflict between the bank register and the Charter when it comes to both storing and sharing of personal data. For the storing of personal data, the AML Directives together with the GDPR and the LED, does not limit the storing clearly in relation to type of information, retention period and the persons affected. The sharing of personal data is problematic as the purposes of the access are unclear might not constitute a fight against serious crime. Furthermore, there are no clear and precise conditions that specify what should be regarded as necessary for access and the sharing is not subject to proper safeguards in terms of a prior review. The result is a high risk for abuse by the authorities with access. These problems indicate that storing and sharing personal data in the bank register is not limited to what is considered strictly necessary for an interference of articles 7 and 8 of the Charter. Safeguards against the misuse by unauthorised third parties seems, however, to be in line with the protection in the Charter regarding both types of processing.
5 Conclusion and Final Remarks

The objective of this thesis was to highlight potential conflict between the requirement to introduce bank registers in all MS and the protection of personal data in the EU. A couple of such potential conflicts have been identified between the AML Directives and the GDPR and the LED, as well as between these frameworks and the rights to protection of personal data and private life in the Charter.

The overall problem with the provisions regulating the bank register seems to be that they are too vague. From the first research question, one could learn that the bank register is a new kind of processing in the sense that it allows for an extensive picture of an individual’s economic engagement, which also allows for extensive conclusions about that individual’s life to be drawn. It was also showed that the possibility to access that information is very broad for FIUs and other authorities, and that the purpose of their access not always is specified. These general provisions were problematic in relation to the GDPR and the LED, because it became unclear for what purpose the data is processed and when the processing is proportional to fulfil that purpose. These problems are foremost in conflict with the principles of purpose limitation, data minimisation and storage limitation. In regard to the Charter, the general character also constitutes the main problem as case law requires that the processing is limited, in terms of the purpose, persons affected, type of data etc., to what is strictly necessary. These conflicts exist even in regard to restrictions on the processing in the bank register imposed by the GDPR and the LED, since the Charter requires the processing to be limited more than these two frameworks do. Furthermore, the CJEU poses strict criteria on safeguards against abuse, such as a requirement for prior review, which neither of the AML Directives, the GDPR and the LED pose, why the bank register in this regard also is problematic.

On 11 July 2019, Directive 2019/1153326 that lays down more specific rules for the use of financial information to fight crime was published. It provides some new rules regarding the access to information in the bank register. An initial glance gives some hope of new rules that can solve some of the issues highlighted in this thesis, for example limitations on the access to certain information and conditions for the access by some authorities. At the same time though, Directive 2019/1153 seems to leave a lot to be

326 Directive 2019/1153 laying down rules facilitating the use of the financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.
desired in terms of the clarity of the purposes of the processing. Without a thorough examination though, it is hard to tell what difference Directive 2019/1153 truly makes.

The conflicts that have been identified in this thesis are particularly problematic because they open up for a general application that entails a high risk of abuse. The abuse that is referred to here is not that the register will be spread to unauthorised third parties, the bank register seems to not only be sufficient in this regard but actually is particularly beneficial. Instead, the problem is the freedom of the FIUs and competent authorities to determine how they can use the information. The authorities can, for example, use the information in ways not intended. This risk of abuse is serious, because it poses a threat to the confidence of the legal system. If that threat is to be realised, we would lose both our liberty and the fundamental system that is keeping us safe.
Bibliography

Treaties

Charter of Fundamental Rights of the European Union, 26 October 2012

Consolidated Version of the Treaty on European Union, 9 May 2008


European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950

Legislation


Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC


Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

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


Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters


Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

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


Skattebrottslag (1971:69)

Cases

**Court of Justice of the European Union**

Joined Cases C-203 & 698/15, Tele2 Sverige AB v. Post- och telestyrelsen, and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis, Judgment of the Court (Grand Chamber) of 21 December 2016

Case C-362/14, Maximilian Schrems v. Data Protection Commissioner, Judgment of the Court (Grand Chamber) of 6 October 2015

Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication, Judgment of the Court (Grand Chamber) of 8 April 2014

Case C-355/10, European Parliament vs Council of the European Union, Judgment of the Court (Grand Chamber) of 5 September 2012
Joined Cases C-92/09 and C-93/09, Volker und Markus Scheke BgR and Hartmut Eifert v. Land Hessen, Judgment of the Court (Grand Chamber) of 9 November 2010

Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, Judgment of the Court of 20 May 2003

Case 79/77, Kuhlhaus Zentrum AG v. Hauptzollamt Hamburg-Harburg, Judgment of the Court (First Chamber) of 9 March 1978

European Court of Human Rights

Zakharov v. Russia, Application no. 47143/06, Judgment of 4 December 2015

M.N. and Others v. San Marino, Application no. 28005/12, Judgment of 7 July 2015

S. and Marper v. the United Kingdom, Applications nos. 30562/05 and 30566/04, Judgment of 4 December 2008

Amann v. Switzerland, Application no. 27798/95, Judgment of 16 February 2000

Leander v. Sweden, Application no. 9248/81, Judgment of 26 March 1987

Silver and Others v. the United Kingdom, Application nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Judgment of 25 March 1983

Literature


Quintel, Teresa, *Follow the money, if you can: Possible solutions for enhanced FIU cooperation under improved data protection rules*, University of Luxembourg, Law Working Paper Series, Paper no. 2019-1


Other Sources


Promemoria Fi2018/03025/B, *Genomförande av 2018 års ändringsdirektiv till EU:s fjärde penningtvättsdirektiv*, Published on 5 September 2018