THE FIGHT AGAINST TERRORISM: A FREE CARD TO SET ASIDE THE FUNDAMENTAL EU DATA PROTECTION RULES?

The compatibility of the draft 5th AML Directive in the light of the EU data protection framework

LLM Paper
by Hanne De Vos
Student number: 01207696

Promoter: Prof. dr. Antoinette Verhage
Co-promotor: Prof. dr. Eva Lievens
PREFACE

First of all, I wish to show my greatest appreciation and gratitude to my promotor, Prof. dr. Antoinette Verhage and co-promotor, Prof. dr. Eva Lievens, for having given me, in such an enthusiastic manner, the opportunity to write this thesis. Getting more acquainted with both the Union’s data protection framework and the AML legislation proved to be a highly interesting and instructive experience, which will most definitely provide some useful guidance throughout my future career.

Secondly, I would like to seize this opportunity as well to send all of my love to my friends and family, as their ongoing support, advice and encouragement appeared crucial to reach the end point of this thesis and the LL.M in general. Writing this dissertation in combination with the demanding LL.M program turned out to be challenging and I honestly do not believe I would have made it without their endless willingness to boost me with much needed motivation speeches.
# TABLE OF CONTENTS

**GENERAL INTRODUCTION** ........................................................................................................... 1

**CHAPTER I. THE EU DATA PROTECTION FRAMEWORK** .................................................................. 4

Section 1 : Data protection rules contained in EU primary law ............................................................... 5

1. Articles 7 and 8 EU Charter .............................................................................................................. 5

2. Article 52(1) of the EU Charter ...................................................................................................... 6

3. Article 16 TFEU ................................................................................................................................ 6

Section 2 : Data Protection rules contained in Article 8 ECHR .............................................................. 7

Section 3 : Data Protection rules contained in EU secondary law ......................................................... 8

1. Directive 95/46/EC and its history ................................................................................................... 8

2. The GDPR and its future ................................................................................................................ 9

   (1) Scope of application ................................................................................................................ 10

   (2) The key Data Protection Principles ......................................................................................... 10

      a. The principle of lawful processing ....................................................................................... 10

      b. The principle of purpose limitation ...................................................................................... 13

      c. The principle of data minimisation ....................................................................................... 15

      d. The principle of data accuracy ........................................................................................... 16

      e. The principle of storage limitation ....................................................................................... 16

      f. The principle of data integrity and confidentiality (data security principle) ....................... 17

      g. The principle of accountability ........................................................................................... 18

   (3) Conclusion .................................................................................................................................. 18

Section 4 : Relevant case law of the Court of Justice of the European Union ...................................... 19

1. Joined cases Digital Rights Ireland and Seitlinger and Others ......................................................... 19

   (1) Facts of the case .................................................................................................................... 20

   (2) Ruling of the Court ................................................................................................................ 21

2. Tele2 Sverige AB and Watson and Others ..................................................................................... 23

   (1) Facts of the case .................................................................................................................... 23

   (2) Ruling of the Court ................................................................................................................ 24

3. PNR Canada (Opinion 1/15) ......................................................................................................... 26

   (1) Facts of the case .................................................................................................................... 27

   (2) Ruling of the Court ................................................................................................................ 27

Conclusion ........................................................................................................................................... 33

Conclusion EU Data Protection Framework ............................................................................................ 34

**CHAPTER II: COMPATIBILITY OF THE DRAFT FIFTH AML DIRECTIVE WITH THE EU DATA PROTECTION FRAMEWORK** .................................................................................. 35

Section 1 : Outline of the draft 5th AML Directive .............................................................................. 35

1. Ratio and envisioned changes ...................................................................................................... 36

2. Scope ratione personae of the AML Directive .............................................................................. 38

3. Data processing obligations imposed by the draft 5th AML Directive ......................................... 39
(1) Customer due diligence measures

<table>
<thead>
<tr>
<th>a. Collection of customer identification data</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.i. Transactions subjected to customer due diligence measures</td>
<td>40</td>
</tr>
<tr>
<td>a.ii. General Customer due diligence information</td>
<td>41</td>
</tr>
<tr>
<td>a.iii. Simplified customer due diligence information</td>
<td>43</td>
</tr>
<tr>
<td>a.iv. Enhanced customer due diligence information</td>
<td>43</td>
</tr>
<tr>
<td>b. Retention of the customer identification data</td>
<td>44</td>
</tr>
<tr>
<td>c. Access to and disclosure of the customer identification data</td>
<td>45</td>
</tr>
</tbody>
</table>

(2) Beneficial ownership information

| a. Collection of beneficial ownership data | 46 |
| b. Retention of the beneficial ownership data | 46 |
| c. Access to and disclosure of the beneficial ownership data | 47 |

Conclusion

Section 2: Assessment of the draft 5th AML Directive in the light of the EU data protection framework

1. Interference with the fundamental rights to privacy and data protection

2. Justification of the found interference

   (1) Legal basis
   (2) Respect the essence of the fundamental rights and freedoms
   (3) Serving objectives of general interest
   (4) The principle of proportionality
       a. Appropriateness of the data processing
       b. Strict necessity of the data processing
       b.i. Collection and retention of personal data provided for by the draft 5th AML Directive
       b.ii. Access to and use of the collected personal data
       b.iii. Purpose limitation principle

Conclusion

FINAL CONCLUSION

BIBLIOGRAPHY

ANNEX: LIST OF DEFINED TERMS
GENERAL INTRODUCTION

1. In these times of terrorism and the keenly-felt climate of fear that comes along with it, initiatives to prevent any further dreadful events from happening generally follow each other at a high pace. Panic bursts out, rapidly affects the minds of each and every one of us, including those of the competent European and national legislators, and incites these latter to undertake often hasty and ill-deliberated action. Along these lines, the European Commission has reacted to the recent and continuing attacks of terrorist organization ‘ISIS’ by – *inter alia* – submitting, on the fifth of July 2016, a proposal to reinforce and expand Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, commonly referred to as the 4th AML Directive.

The Council and Parliament of the European Union subsequently engaged in interinstitutional negotiations with the Commission, which resulted in a provisional agreement pertaining to this proposed revision [hereinafter, the ‘draft 5th AML Directive’]. The text agreed upon, in the meantime adopted by the Parliament in first reading on 19 April 2018, envisions improving the fight against terrorist financing and money laundering by (further) strengthening the transparency rules concerned. The draft 5th AML Directive primarily aims to ascertain full insight in the ownership of companies and trusts by substantially enhancing access to the relevant information thereof, as well as to monitor new means and channels of terrorist financing (see no. 77).

---

1 Islamic State of Iraq and Syria, also known as ISIL (Islamic State of Iraq and the Levant).
2. However, it is crucial to make sure that our generalized fear of terrorism does not blind us from the potential dangers the foreseen higher level of transparency entails in terms of privacy and data protection. As recent scandals (e.g. Cambridge Analytica) have clearly demonstrated, (unlawful) large-scaled collection and further processing of personal data too can have serious repercussions, likewise assuming global proportions.⁷

In view of protecting individuals against this second category of threats as well, it must be noted that the European Union has, since 1995⁸, joined its forces to build a decent and quite elaborated ‘data protection framework’, which it equally continues to reinforce. This framework sets out a number of principles, conditions and safeguards that data controllers and processors need to abide by when engaging in the processing of one’s personal data. Needless to say, those rules can only live up to their expectations when fully honoured by both the Member States and the Union institutions themselves. Where the draft ⁵th AML Directive, to the contrary, primarily focuses on completely exposing the Union’s financial system and monitoring approximately all of its players, the required respect for the provisions referred to seem, however, not at all self-evident.

3. Accordingly, the aim of the presented dissertation is to examine whether and to what extent the proposed draft ⁵th AML Directive has succeeded in pursuing its objective of preventing and detecting terrorist financing and money laundering offences while taking into account the Union’s vital data protection regulations. In other words, the research conducted in the context of this thesis essentially aims at verifying whether the envisioned draft ⁵th AML Directive is compatible with the Union’s fundamental rights to privacy⁹ and data protection¹⁰ as interpreted by the CJEU, as well as with related principles in the General Data Protection Regulation [hereinafter: ‘GDPR’].¹¹ The relevance and urgency of this research question cannot be underestimated as the unlawful collecting and further processing of personal data based on the draft ⁵th AML Directive – considering its drafting is entering into a final stage – would expose us all to dangers we cannot even try to understand yet at this point.

---

⁷ It is claimed that both the ‘Brexit’ and the current President of the United States owe their presence to the unlawful processing of approximately 87 million of data subjects: ‘The Cambride Analytica Files’ (The Guardian) <https://www.theguardian.com/news/series/cambridge-analytica-files> accessed 23 April 2018.
¹⁰ EU Charter, Art. 8.
In order to provide an answer to the posed question, first, the Union’s data protection framework will be set out and clarified (Chapter I). Thereafter, this thesis will continue by assessing the compatibility of the draft 5th AML Directive with the discussed provisions and principles (Chapter II). To that end, the draft 5th AML Directive will in a first section briefly being outlined (section 1) and will subsequently be scrutinized in the light of chapter II (section 2). Finally, a conclusion will be provided as to whether the draft 5th AML Directive succeeded in reaching a reasonable balance between, on the one hand, its aim to combat terrorist financing and money laundering by increasing transparency and, on the other hand, the need to safeguard the data subjects affected by it against the unlawful processing of their personal data.

The ultimate answer will determine whether the EU Parliament and Council can rightfully proceed with the adoption of the draft 5th AML Directive in its current form, or whether the competent Union institutions should, on the contrary, seek the courage to make some last-minute amendments to the latter instrument in order to ascertain compliance with the Union’s data protection framework.
CHAPTER 1. THE EU DATA PROTECTION FRAMEWORK

5. The digital age we live in creates, next to a number of valuable opportunities and world-changing innovations, also an utmost vulnerable environment in which a high number of individuals can simultaneously be monitored and be subject to, sometimes quite intrusive, forms of collecting and processing of their personal data. The undeniable need for data subjects to be protected against unlawful forms of such processing, and to have a certain level of control with regard to their personal data, has moved the European Union to develop its own legal framework for data protection.

6. The mindfulness with which the Union has assumed this office and the importance it attached to protecting the privacy and personal data of its citizens, is clearly evidenced by the presence of EU data protection provisions and principles at every level of EU law (primary law, secondary law, case law and soft law measures).

First of all, Articles 7 and 8 of the EU Charter, that since the coming into force of the Lisbon Treaty in 200912 is endowed with the same binding value as the EU Treaties13, guarantee the fundamental rights to respect for one’s private life and to the protection of one’s personal data. Both fundamental rights represent of course a central place in the Union’s data protection framework and will therefore be heavily discussed in the presented dissertation (see no. 8-11).

Pertaining to the level of secondary law, the legal instrument that is the most relevant for the presented thesis is the recently much brought up ‘GDPR’, entering into force on the 25th of May 2018 as successor of the currently applicable Data protection Directive. The GDPR seeks to reinforce a number of key ‘data protection principles’ and to further elaborate on the rights that are offered to the data subjects affected to exercise a certain control on the processing of their personal data (see no.19-42).

Thirdly, also the CJEU (and to a certain extent the European Court of Human Rights [hereinafter: ‘the ECHR’]) have made an important contribution to the development of the Union’s data protection framework as well, by interpreting and clarifying the fundamental rights to privacy and data protection contained in the EU Charter and the key principles contained in the mentioned secondary EU law (see no. 43-70).

7. In the following section, each of these building stones will enjoy a more in-depth discussion, as they appear crucial for the assessment this thesis aims to carry out. It must be noticed that countless soft-law instruments are issued as well in view of clarifying the said data protection framework. However, due to the limited length of the presented dissertation, these additionally measures will not be addressed.

Section 1: Data protection rules contained in EU primary law

1. Articles 7 and 8 EU Charter

8. The EU rightfully deemed the protection of personal data to be so vital that it included, as the first and sole institution to date\textsuperscript{14}, a distinct right to the protection of personal data next to a fundamental right to private life, into its Charter of Fundamental Rights (resp. Articles 8 and 7)\textsuperscript{15}, obliging all Member States implementing EU law and each and every institution, body, office and agency of the Union itself to, fully and at all times, respect both fundamental rights.\textsuperscript{16}

Article 7 of the Union’s Charter ("respect for private and family life") reads as follows: “Everyone has the right to respect for his or her private and family life, home and communications”. Whilst Article 8, titled the “protection of personal data”, provides that: “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority”.

9. Hence, Article 8 of the EU Charter preserves, next to an explicit right to data protection, also the most essential elements of the Data Protection Directive (such as the key principles of lawful processing and purpose limitation, and the rights granted to data subjects’ to access and rectification), and subsequently elevates these elements to the level of EU primary law, directly applicable in all Member States.\textsuperscript{17} Accordingly, when one’s personal data are being processed with


\textsuperscript{16} Article 51(1) EU Charter; Peter Hustinx, ‘EU Data Protection Law’, 20.

\textsuperscript{17} Explanatory Notes to the Charter of Fundamental Rights of the European Union, Convent 49 (11 October 2000), explanation on Article 8, 10-11 \texttt{<http://www.europarl.europa.eu/charter/convent49_en.htm>} accessed 3 April 2018;
disregard of the most crucial data protection aspects, a violation of his or her fundamental right to data protection, enhanced in Article 8 of the EU Charter, will clearly rise.

10. As Articles 7 and 8 of the EU Charter constitute the heart of the Union’s data protection framework, both provisions will enjoy particular attention when assessing the compatibility of the draft 5th AML Directive with it.

2. Article 52(1) of the EU Charter

11. Notwithstanding the vital importance of the quoted rights to respect for privacy and data protection, these rights are not absolute. In the same way as the other fundamental rights and freedoms of the EU Charter, they are subject to the general derogation clause contained in Article 52(1), which allows for limitations when four conditions are met. Subsequently, the relevant rights to privacy and data protection may be interfered with provided that this interference is, first of all, described by law; respects the essence of the fundamental rights and freedoms; follows an objective of general interest recognised by the Union (or aims to protect the rights and freedoms of others); and finally appears proportional to its expressed objectives.

The CJEU’s case law demonstrates that when practices of personal data processing are questioned, the focus will consistently lie on the fulfilment of the derogation clause, and more particularly on the proportionality test contained within it (see no.43-70). The same shall apply with regard to the processing of personal data based on the draft 5th AML Directive.

3. Article 16 TFEU

12. Lastly, it must be noticed that also the Treaty on the Functioning of the European Union [hereinafter: ‘TFEU’] guarantees in its Article 16(1) that: “everyone has the right to the protection of personal data concerning them.” However, following the CJEU’s approach, the focal point of the presented dissertation shall lie on the right to data protection embodied in Article 8 of the EU Charter, which is indeed provided in a more elaborated fashion.

Nevertheless, the value of Article 16(2) TFEU can on the other hand not be belittled, as this provision endows the European Parliament and Council explicitly with a general legal basis for the further

---


adoption of rules relating to the protection of personal data, as well as to the free movement of such data.\textsuperscript{20}

\textbf{Section 2: Data Protection rules contained in Article 8 ECHR}

\textbf{13.} Although it is the intention of the presented dissertation to examine the compatibility of the draft 5\textsuperscript{th} AML Directive with EU data protection laws, a brief discussion of the right to respect for private and family life, embodied in Article 8 ECHR, cannot be left out.\textsuperscript{21}

Since 1950, Article 8, §1 ECHR ensures that: “\textit{everyone has the right to respect for his private and family life, his home and his correspondence}”. Derogations hereof can only be accepted when they are in accordance with the law and appear necessary in a democratic society to achieve a limitative number of legitimate interests.\textsuperscript{22}

This well-developed right to privacy has been the number one provision to invoke when a person’s privacy gets, in any way, endangered and the case law of the European Court for Human Rights has made clear that this includes cases in which one’s personal data was processed in an unlawful manner. Indeed, the quoted Court repeatedly reiterated that the protection of one’s personal data were “of fundamental importance for a person’s enjoyment of the right to respect for private”.\textsuperscript{23}

Accordingly, adopting a careless attitude towards the processing of personal data is likely to result in a violation of Article 8 ECHR as well, subject to the inspection of the European Court of Human Rights.

\textbf{14.} Moreover, Article 8 ECHR shows to be of particular importance with regard to EU data protection law because of the reference that is being made in Article 52(3) of the EU Charter, which states that “\textit{in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the said Convention}.”\textsuperscript{24} In other words, the interpretation the European Court of Human Rights adopted

\textsuperscript{20} However, it must be clear that the scope of this horizontal legal basis exceeds that of the internal market and provides for protection in principally all EU policy areas, regardless of whether this relates to the internal market: Peter Hustinx, ‘EU Data Protection Law’, 19.

\textsuperscript{21} Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 5 ['ECHR'].

\textsuperscript{22} ECHR, Art. 8, §2.

\textsuperscript{23} See, \textit{inter alia}, Klass v Germany App no 5029/71 (ECtHR, 6 September 1978); Malone v United Kingdom App no 8691/79 (ECtHR, 2 August 1984); Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987); Gaskin v United Kingdom App no 10454/83 (ECtHR, 7 July 1989); Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992); Halford v United Kingdom App no 20605/92 (ECtHR, 25 June 1997); Amann v Switzerland App no 27798/95 (ECtHR, 16 February 2000) and Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000); Peter Hustinx, ‘EU Data Protection Law’, 7. See also: European Union Agency for Fundamental Rights (FRA), \textit{Handbook on European data protection law} (Publications Office of the European Union 2014) 20 ['Handbook on European data protection law'].

pertaining to the right to privacy - and to the right to the protection of personal data contained therein - is of vital importance in determining the impact of the rights to privacy and data protection as harboured in the EU Charter.

**Section 3: Data Protection rules contained in EU secondary law**

15. At a second level, the specific principles and conditions which must be taken into account when processing personal data, the safeguards that ought to be inserted and the rights that need to be given to the data-subjects, are in a more detailed way described in EU secondary law.

1. Directive 95/46/EC and its history

16. Today the quoted substantive EU data protection rules are enshrined in Directive 95/46/EC (‘the Data Protection Directive’). The European Parliament and Council adopted this Directive in 1995 and followed hereby the double objective to, on the hand, oblige the Member States to protect their citizens’ personal data, and to, on the other, require them neither to restrict, nor to prohibit, the free flow of personal data amongst each other for reasons connected with such protection.  

17. However, it was in fact the Council of Europe that, by adopting the Data Protection Convention (also known as ‘Convention 108’) for the first time in 1981 gave existence to the data protection principles and put data protection on the agenda. Later, the Data Protection Directive then used the realizations of Convention 108 as a starting point and supplemented these with further requirements and conditions. In doing so, the EU primarily strived to harmonise the national laws on data protection in both the private and (most parts of) the public sector, ensuring more consistency across the EU.

To a considerable extent, the Directive genuinely succeeded in its object and introduced a number of vital EU data protection principles widely across the Member States, which subsequently have taken up an important position. However, as the concepts in the Data Protection Directive are formulated in rather general wording and still left the Member States a broad margin of appreciation to

---

28 Commission, ‘Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security’ COM(90) 314 final.
transpose them, the absence of a fully consistent national data protection framework prevailing in all Member States was still regretted.\(^{29}\)

18. Accordingly, the currently applicable Data Protection Directive constitutes, in turn, the subject of a wide-ranging review, which will –after four years– be completed on the 25\(^{\text{th}}\) of May 2018 with the coming into force of the already famous GDPR.\(^{30}\) In this view, the key EU data protection principles, which are to be considered a second series of cornerstones composing the Union’s data protection framework, will be discussed under the following title, pertaining to this latter instrument. Adjustments as compared to their current existence under Directive 95/46/EC, which are certainly not overwhelming, will consistently be indicated.

2. The GDPR and its future

19. Hence, within a few days the GDPR will become the Union’s number one tool to refer to when dealing with the collection and further processing of personal data, as it will provide a reinforced and elaborated outline of the Union’s key data protection principles and other safeguards. In this view, its vision to both strengthen Union citizens’ rights to the protection of their personal data, which is much needed in the digital age we live in, and to enhance the internal market dimension, abolishing the Member States’ hesitation to transfer duly gathered personal data to other Member States, has certainly been welcomed.\(^{31}\) Furthermore, also the fact that the Regulation, as opposed to the Directive, will be directly binding in all Member States and therefore anticipates a stronger implementation and respect for the quoted principles has been praised as a 'huge step forward' towards a more effective and consistent protection of personal data across the Union’s territory.\(^{32}\)

In view of the important role the GDPR will play, the presented dissertation will, after providing a short outline of its scope (no. 20-21), offer an in-depth discussion of the said EU data protection principles (no19-42). It must be noted that the GDPR also aims to strengthen the rights granted to the data subjects. However, given the limited length of this thesis, a discussion thereof must be left out.

\(29\) GDPR, rec. 9. Additionally, the Commission considered that the current rules on data protection needed to be modernised in light of rapid technological developments and globalisation as well: Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ COM(2012) 11 final [‘Proposal GDPR’].

\(30\) GDPR, Art. 99.


\(32\) GDPR, rec. 10; Press release EDPS; Peter Hustinx, ‘EU Data Protection Law’, 29.
(1) **Scope of application**

20. The GDPR is applicable to all processing of personal data that is wholly or partly conducted by automated means or by other means related to a filing system.\(^{33}\) In other words, the GDPR is endowed with a general scope and covers both the private and public sector, as well as all contexts and all fields within these sectors as soon as they touch upon the processing of personal data.\(^{34}\) Furthermore, the protection offered is technologically neutral.\(^{35}\)

With a view to counter the holistic approach used by the GDPR, Article 2(2)-(3) lists a number of activities that are, although they constitute the processing of personal data, excluded from its scope. However, as none of these exclusions apply to the processing of personal data imposed by the draft 5\(^{th}\) AML Directive, a further explanation hereof will be left out.

21. Secondly, with regard to the GDPR’s scope *ratione territoriae*, it is noteworthy that the Regulation applies to the same entities that are covered by the draft 5\(^{th}\) AML Directive, since both EU instruments apply to activities carried out by entities established within the Union.\(^{36}\)

(2) **The key Data Protection Principles**

22. The GDPR explicitly lists a total of seven principles that it considers fundamental to abide by when processing one’s personal data.\(^{37}\) Each of these principles encompass, although all interconnected, a specific intention that contributes to the data subjects’ protection.

a. **The principle of lawful processing**

23. The first principle mandates that the processing of personal data must be carried out “*lawfully, fairly and in a transparent manner in relation to the data subject*”.\(^{38}\) Accordingly, already three forms of data protection are essentially ensured.

24. First of all, in response to the complexity that often accompanies data processing practises and makes it difficult for citizens to understand the impact thereof, the principle demands for transparency.\(^{39}\) Data processors must make it clear to natural persons that their personal data are collected, used, consulted or otherwise processed and must subsequently provide them with

---

\(^{33}\) GDPR, Art. 2(1)

\(^{34}\) Peter Hustinx, ‘EU Data Protection Law’, 30.

\(^{35}\) GDPR, rec. 15.

\(^{36}\) GDPR, Art. 3(1).

\(^{37}\) GDPR, Art. 5(1).

\(^{38}\) GDPR, Art. 5(1)(a).

\(^{39}\) Handbook on European data protection law, 73-75.
relevant information about such processing, in an accessible and fully understandable way. In particular, data subjects must be informed about the identity of the controller, the purposes of the processing, the sorts of data that are being obtained and how they are being obtained, the storage period, the risks, and lastly, data subjects should be offered information on how they can execute the rights granted by the GDPR.\textsuperscript{40}

25. Secondly, the quoted first key principle warrants the lawfulness of the processing of personal data, as it only allows processing that is in accordance with the law, albeit in the broad sense of the word.\textsuperscript{41} In this regard, a reference needs to be made to Article 6(1) GDPR, which sets out six limited conditions under which the processing of personal data is considered lawfully.

First of all, the processing of personal data can lawfully be based on the data subject’s consent, given for a specific purpose.\textsuperscript{42} However, the drafters of the GDPR clearly indicated to only consider a person’s ‘consent’ valid if, and to the extent that, such consent is (a) freely given\textsuperscript{43}, (b) specific, (c) informed and (d) unambiguous.\textsuperscript{44} Accordingly, in order to rely on this legal basis, the data subject must genuinely have chosen to allow the processing of his or her data for each and every of the purpose(s)\textsuperscript{45} that were previously explained by the data controller. Furthermore, also the conditions contained in Article 7 of the GDPR must be fulfilled, as well as the prerequisite of parental consent or authorization in case the data subject is younger than 16 years of age.\textsuperscript{46}

Secondly, even without an (explicit) consent, the processing of personal data will be considered lawfully when such is necessary for the performance of, or the entrance in, a contract to which the data subject is a party.\textsuperscript{47}

Of greater importance in the light of the presented dissertation, is the third possible legal ground which entails the (conditional) permission to process personal data when such is “necessary for compliance with a legal obligation [in national or EU law] to which the controller is subject”.\textsuperscript{48} The legal ground to process personal data \textit{because one has to}, is the ground most often used by data

\textsuperscript{40} GDPR, rec. 39.
\textsuperscript{41} Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament: GDPR, rec. 41.
\textsuperscript{42} GDPR, Art. 6(1)(a).
\textsuperscript{43} GDPR, rec. 43.
\textsuperscript{44} GDPR, rec. 31.
\textsuperscript{45} When the processing has multiple purposes, consent should be given for all of them. Moreover, if a controller wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose: GDPR, rec. 32.
\textsuperscript{47} GDPR, Art. 6(1)(b).
\textsuperscript{48} GDPR, Art. 6(1)(c).
controllers acting in the private sector, including a large part of the companies targeted by the draft 5th AML Directive.\footnote{Handbook on European data protection law, 82. However, the legal obligation must be binding in nature: Detlev Gabel and Tim Hickman, ‘Unlocking the EU General Data Protection Regulation’ [2016], Chapter 7 <https://www.whitecase.com/publications/article/chapter-4-territorial-application-unlocking-eu-general-data-protection#toc> accessed 26 April 2018 [‘Unlocking the EU General Data Protection Regulation’].} In this respect it is important to keep in mind that both the Union institutions and the Member States can fairly introduce such legal grounds (laws), provided that they meet an objective of public interest to which they are proportionate.\footnote{GDPR, rec. 45.} Furthermore, the GDPR requires that the purpose of the processing is determined in that legal basis\footnote{GDPR, Art. 6(3).}, but allows that one law serves as a ground for several processing operations based on the legal obligation to which the controller is subject.\footnote{GDPR, rec. 45.}

The fourth ground on which data processing can ‘lawfully’ be based pertains to the need to process personal data in order to protect the vital interests of the data subject or other natural persons.\footnote{GDPR, Art. 6(1)(d).} As ‘vital interests’ are considered to be closely related to the life and survival of the data subject, this basis mostly serves as a ground for the legitimate use of health data or of data about missing persons, for instance.\footnote{GDPR, rec. 46; Handbook on European data protection law, 83.}

Furthermore, Article 6(1)(e) GDPR allows data processing when such is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, again within the Union or a Member State.\footnote{GDPR, Art. 6(3) and rec. 45.} This legal ground enables Member States to efficiently organize various public affairs.

Lastly, the GDPR allows the processing of personal data necessary to safeguard “\textit{legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data}”. When the data subject is a child, special precaution is required.\footnote{GDPR, Art. 6(1)(f).} Hence, in order to rely on this legal ground, a two-steps process has to be passed through. Firstly, the legitimate interests of the data controller (or of a third party) have to be identified, and secondly, they have to be balanced against the interests, fundamental rights and freedoms of the data subject itself.\footnote{This ground does not apply to processing carried out by public authorities in the performance of their tasks: GDPR, rec. 47. Moreover, processing carried out on this basis may be subject to objections from data subjects: Unlocking the EU General Data Protection Regulation, Chapter 9.}
Practise under the current Directive 95/46/EC exhibits however a narrow approach, which will most probably be continued under the future GDPR as well.\textsuperscript{57}

26. Before closing the discussion on the first key data protection principle, the existence of some ‘special categories of personal data’ still needs to be highlighted. These categories, referred to as ‘sensitive data’, are listed in Article 9(1) of the GDPR and are subject to additional conditions in order for their processing to be lawful. Essentially, the approach followed by the GDPR (in compliance with the current Directive 95/46/EC)\textsuperscript{58} prohibits the processing of these sensitive data, unless, and to the extent that, at least one of the exception grounds provided in Article 9(2) GDPR, together with the therein-contained conditions, can be demonstrated.

27. Along the same lines, also the processing of personal data pertaining to criminal convictions and offences, or related security measures, are subject to additional safeguard provisions. It is to say, such processing can only be considered lawfully when proceeded under the control of an official authority or when the processing is authorised by Union or Member State law, which provides for appropriate safeguards for the rights and freedoms of data subjects. Additionally, any comprehensive register of criminal convictions may be kept solely under the control of an official authority.\textsuperscript{59}

Both categories of ‘special’ personal data appear to be relevant for the assessment carried out by the presented thesis.

28. Finally, it must be clear that the principle of lawful processing holds an apparent link with the derogation clause embodied in Article 52(1) of the EU Charter, as this provision governs the conditions in which limitations to the fundamental rights to privacy and data protection can be considered ‘lawful’. In this view, a reference is made to paragraph 11.

b. The principle of purpose limitation

29. The second EU data protection principle demands ‘purpose limitation’ and should undeniably be regarded as a cornerstone of the Union’s entire data protection framework.\textsuperscript{60} As the Article 29 Working Party concisely elucidated, the first step of duly data processing must always be the

\textsuperscript{57} See: Unlocking the EU General Data Protection Regulation, Chapter 7.
\textsuperscript{58} Directive 95/46/EC, Art. 8.
\textsuperscript{59} GDPR, Art. 10.
\textsuperscript{60} The purpose limitation principle is also implied in Article 8(2) of the EU Charter (see no. 10).
specification of the pursued purposes.61 Subsequently, the other data protection principles ought to build further upon the expressed purposes.

30. More particularly, the purpose limitation principle requires that “personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”.62 Hence, the principle essentially encompasses two components.

In a first phase of data collection, it compels the data controller to carefully and precisely assess what purpose(s) the personal data will be used for, to ensure that these are in accordance with the law63 and to subsequently reveal, explain or express the set out purposes in an intelligible form.64 The processing of personal data for undefined and/or unlimited purposes is thus unequivocally unlawful.

In a second phase, once the data are collected, the principle prohibits data controllers to use them in a way that is incompatible with the initially defined purposes. Hence, every (new) purpose that a data controller seeks to pursue by using the gathered personal data must have its own particular and demonstrated legal basis, as soon as it is considered incompatible with the original purposes. In order to decide whether an additional purpose is (in)compatible, Article 6(4) GDPR provides a non-exhaustive list of factors that should be taken into consideration.65 Moreover, the Regulation explicitly considers further processing for certain archiving or statistical purposes not to be incompatible with the initial purposes, whatever they are.66 For the remainder the concept of ‘compatibility’ is, however, left open to interpretation on a case-by-case basis.67

31. On the other hand, it must be said that Article 6(4) of the GDPR preserves some room for exceptions as well, in which the further processing of collected personal data is allowed even when the additional purposes pursued are incompatible with the initial ones. In view of the importance of the purpose limitation principle, these (two) exceptions can certainly not be disregarded. Firstly, the further processing of gathered personal data is, in principle, allowed when such is based on the data

62 GDPR, Art. 5(1)(b).
63 In particular, the purposes must be based on one of the mentioned legal grounds listed in Article 6(1) GDPR: Working Party 29 WP203, 19-20.
64 This should happen no later than the time when the collection of personal data starts: GDPR, rec. 39. Moreover, an intelligible form requires a declaration to the appropriate supervisory authority or, at the least, internal documentation that is made available to both the supervisory authorities and the data subject: Handbook on European data protection law, 68.
65 GDPR, rec. 50; Working Party 29 WP203, 23-27.
66 GDPR, Article 5(1)(b); Working Party 29 WP203, 28.
subject's consent. Secondly, the same applies to the further use of collected data when such relies on an EU or Member State law “which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) GDPR”. The objectives in question include, *inter alia*, national security; the prevention, investigation, detection or prosecution of criminal offences; and important economic or financial interests of the EU or a Member State, such as taxation matters.

32. Accordingly, the purpose limitation principle is designed to establish the boundaries within which personal data can be collected and put to further use, and will be one of the crucial factors in determining the legitimacy of the data processing concerned. Along these lines, this second key principle is, as well as the permissible exceptions thereon, from upmost importance with regard to the presented dissertation (see no. 128-131).

c. The principle of data minimisation

33. The third EU data protection principle, enshrined in Article 5(1)(c) GDPR, harbours the requirement for the processed personal data to be “*adequate, relevant and limited to what is necessary in relation to its purposes*”.

This principle is regarded as ‘the principle of proportionality’ and obliges data controllers to ascertain that the categories of data chosen for processing cover no more than the minimum amount strictly necessary to achieve the lawful and previously defined purpose(s) of the processing operations. Hence, a data controller should only collect data which are directly relevant for the pursued purposes notified to the data subjects. In this respect, it must be pointed out that a clear link exists between the principle of data minimisation embodied in the GDPR and the derogation clause contained in Article 52(1) of the EU Charter, which includes a proportionality principle as well (see no.11).

34. Again, the relevance of this principle, both in the light of the presented dissertation and of the Union’s data protection framework in general, cannot be stressed enough.

---

68 GDPR, rec. 50.
70 In this view, the data minimization principle is also being referred to as the ‘data relevancy principle’: Handbook on European data protection law, 70; Unlocking the EU General Data Protection Regulation, Chapter 7.
d. The principle of data accuracy

35. The data accuracy principle, constituting the fourth EU data protection principle, states that personal data must be “accurate and, where necessary, kept up to date”. Subsequently, it forces data processors and controllers to undertake every reasonable step to immediately erase or rectify personal data that are, on the contrary, inaccurate in view of the purposes for which they are processed.\(^{71}\)

This quality principle seeks to protect data subjects by only allowing the use of their personal information when there is a reasonable degree of certainty that the data are accurate and up to date.\(^{72}\) Especially in situations where a considerable amount of potential damage might be caused to the data subject if data were to remain incorrect, regular checking of the accuracy of data, and subsequently updating where necessary, is therefore deemed vital.

e. The principle of storage limitation

36. The fifth EU data protection principle sets out that identifying data may not “be kept longer than is necessary for the purposes for which the personal data are processed”.\(^{73}\) Briefly put, collected personal data must be erased as soon as the expressed purposes have been served. This ‘data retention principle’ is deemed to be a key factor in ensuring the fair processing of personal data.\(^{74}\)

However, again two nuances must (shortly) be pointed out. Firstly, a longer retention period is allowed when the data are used for archiving purposes in the public interest; for future scientific or historical research; or for statistical use, and provided that special safeguards are introduced. Secondly, the storing limitation principle has only been introduced pertaining to data “kept in a form which permits identification of data subjects”. Accordingly, data that are no longer needed, could, on the other hand, lawfully be stored using anonymization or pseudonymization techniques.\(^{75}\)

37. Together, the data minimization, accuracy and storage limitation principles are referred to as ‘data quality principles’.\(^{76}\) In essence, they require proportionality of the data processing and are to be implemented by the controller in all processing operations.

\(^{71}\) GDPR, Art. 5(1)(d).
\(^{72}\) Handbook on European data protection law, 71.
\(^{73}\) GDPR, Article 5(1)(e).
\(^{74}\) Unlocking the EU General Data Protection Regulation, Chapter 7.
\(^{75}\) GDPR, rec. 29; Handbook on European data protection law, 73.
\(^{76}\) Handbook on European data protection law, 70.
f. The principle of data integrity and confidentiality (data security principle)

38. The sixth EU data protection principle harbours the security, integrity and confidentiality of the gathered and processed data. More specifically, it postulates that “personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage”. In order to do so, the principle further requires the use of appropriate technical or organisational measures.

39. Hence, in the light of the data security principle, data controllers are also responsible for taking sufficient measures capable of protecting personal data against both external (e.g., malicious hackers) and internal threats (e.g. poorly trained employees). The European Data Protection Supervisor [hereinafter: ‘EDPS’] explicitly clarified in this regard that such risks include more than those explicitly mentioned in Article 5(1)(f) of the GDPR. Indeed, next to the listed risks to confidentiality (‘unauthorised processing’), integrity (‘unlawful processing’) and availability (‘accidental loss, destruction or damage’), the processing of personal data can be confronted with other risks (‘all other unlawful forms of processing’), which need to be identified and countered as well.

Such leads to the liability of the data controller (or processor) to firstly evaluate the risks inherent to the concerned processing and to subsequently implement measures to mitigate those risks. In this regard, the level of security (and confidentiality) must be “appropriate” in view of the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. Therefore, the EDPS stressed that the correct identification of such ‘appropriate measures’ necessitates specific frameworks, and referred to the ‘Information Security Risk Management (ISRM) process’ as a suitable example thereof.

---

77 GDPR, Art. (5)(1)(f) and rec. 39 GDPR.
78 Working Party 29 WP4, 6.
79 When the personal data processing is carried out by a processor, the latter must be bound to the controller with a contract or other legal instrument, and may only act on instructions from the controller. Moreover, rules on data security also apply the processor: Handbook on European data protection law, 94. See also in this regard: Working Party 29 WP4, 6.
80 GDPR, rec. 83.
81 Ibid.
83 EDPS Guidance document on security measures for personal data processing, 6-9.
g. The principle of accountability

40. Finally, the last principle set out by the GDPR declares data controllers in general responsible for the compliance with the quoted EU data protection principles.\(^{84}\) According to the Article 29 Working Party, the data controller must, more precisely, put in place measures which –at least under normal circumstances– guarantee that all EU data protection principles are fully respected within their data processing activities.\(^{85}\) A second aspect of the accountability principle subsequently requires data controllers to retain evidence proving the specific measures adopted to fulfil this obligation, and to disclose the kept documentation to data subjects, the general public and the supervisory authorities.\(^{86}\)

Hence, with this finalizing principle, the EU legislator sought to guarantee the enforcement of the other EU Data protection principles in order to effectively promote and safeguard data protection in all processing activities, as well as to provide transparency thereof.

(3) Conclusion

41. The discussed EU data protection principles form the cornerstones of the Union’s data protection framework and encompass, especially in the light of the entering into force of the GDPR, an empowered and elaborated set of conditions with which data controllers have to comply before, during and after the processing of personal data. Primordially these principles demand, as does the EU Charter, the processing of personal data (in all of its aspects) to be limited to what is necessary to achieve the previously and specifically expressed purposes thereby pursued.

42. The EU data protection principles are also relied upon by the CJEU when it assesses measures containing restrictions to the rights laid down in Articles 7, 8 and 52(1) of the Charter. Hence, if the Court were to examine the compatibility of the draft 5\(^{th}\) AML Directive with the Union’s data protection framework, the question whether or not the EU data principles are respected, will play a decisive role.

---

\(^{84}\) GDPR, Art. 5(2), rec. 85.


\(^{86}\) Working Party 29 WP173.
Section 4: Relevant case law of the Court of Justice of the European Union

43. As always, an overview of the CJEU’s most important case law cannot be disregarded, as its ‘interpretations’ are crucial in order to both fully understand and apply EU law correctly. In the context of the processing of personal data, this case law primarily focuses on the permission and justification of restrictions to the quoted fundamental rights to privacy and data protection, embodied in Articles 7 and 8 of the EU Charter. However, since the extent to which derogations to the fundamental rights are allowed is of fundamental importance to determine the level of protection guaranteed by EU data protection law, it must be clear that the following case law, in itself, significantly contributes to the framework against which the draft 5th AML Directive must be examined.

Accordingly, the following section will display three highly important cases that clarify the conditions that, according to the CJEU, have to be fulfilled to justify the processing of one’s personal data.

1. Joined cases Digital Rights Ireland and Seitlinger and Others

44. A first landmark case that the presented dissertation will discuss is the case of “Digital Rights Ireland”, ruled by the Grand Chamber of CJEU on the 8th of April 2014. The Court used this judgement to clarify that restrictions to the fundamental rights to privacy and data protection must always be targeted, both in the initial phases of the ‘collection’ and ‘retention’ of personal data and in the subsequent phases of ‘access to’ and ‘use of’ the gathered data. The fact that the data are being processed in view of combatting serious crime (e.g. terrorism) does not impair this consideration. In Digital Rights Ireland, the Court considered the EU Data Retention Directive not to fulfil these conditions and consequently declared it invalid.

In the following, some more background and clarifications will be provided, as the concrete facts, reasoning and conclusion of the Court will successively be discussed.

87 Gert Vermeulen, ‘The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services’ in Svantesson, Dan J.B. and Dariusz Kloza (eds), Transatlantic Data Privacy Relationships as a Challenge for Democracy; European Integration and Democracy Series, vol 4 (Intersentia 2017), 7 [‘Gert Vermeulen, ‘The Paper Shield’’].
(1) **Facts of the case**

45. The Data Retention Directive aimed at harmonizing Member States’ provisions adopted pursuant to Directive 2002/58/EC (the so-called ‘e-Privacy Directive’)\(^9\), which translates the principles set out in the Data Protection Directive into specific rules for the telecommunications sector. In this light, also Article 15,§1 of the e-Privacy Directive embodies a general exception clause, allowing restrictions to certain therein contained principles that “constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard, amongst others, national security; defence; public security; and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system”.

After being confronted with various different national provisions adopted by the Member States on the ground of the quoted exception clause, which harmed the internal market, the EU introduced the Data Retention Directive.\(^9\) Accordingly, this Directive stated that, for the purpose of the prevention, investigation, detection and prosecution of serious crime - in particular organised crime and terrorism- certain service providers had to retain (an important amount of) traffic and location data, as well as related data necessary to identify the subscriber or user.\(^9\)

46. However, both the Data Retention Directive and the national provisions adopted on its foundation were challenged by the applicants in the case, the Irish organization Digital Rights Ireland Ltd and the Austrian regional government of the Province of Carinthia, which eventually resulted in a preliminary ruling before the CJEU, essentially asking whether the Data Retention Directive was valid in the light of Article 7 (the right to respect of privacy), Article 8 (the right to data protection) and Article 11 of the EU Charter.\(^9\)

---


\(^9\) Data Retention Directive, Art. 1 and rec. 6.


21

(2) Ruling of the Court

47. The Court straightforward ruled that the Directive –in a particularly serious manner– interfered with both the fundamental rights to respect for private life (Article 7) and personal data protection (Article 8). With regard to Article 7 of the EU Charter, the Court more specifically reiterated the fundamental consideration that “it did not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way” in order to establish a violation of the right to privacy.93 With regard to Article 8 of the EU Charter the CJEU subsequently launched a second remarkable and unmistakable message, entailing that the fundamental right to the protection of personal data is interfered with as soon as personal data is being processed.94

48. Consequently, the Court continued its reasoning examining whether the found interferences could be justified. In this regard, it referred to the general exception clause contained in Article 52(1) of the EU Charter, which dissects four distinct conditions, as it provides that “any limitation on the exercise of the rights and freedoms laid down by the Charter must (1) be provided for by law, (2) respect their essence and must (3), subject to the principle of proportionality, be necessary to (4) meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.” As in almost all cases before the CJEU, the Court thereupon found difficulties pertaining to the question of proportionality. Where the CJEU acknowledged that the invoked objectives, in casu the combatting of serious crime, constituted indeed an objective of general interest95, it was on the other hand markedly unconvinced that the envisioned data processing was proportional in the light of these expressed purposes.

49. In this regard, the CJEU highlighted the two components of the proportionality test, which in the presented case firstly required the data processing to be appropriate for attaining the legitimate objectives pursued – which the Court accepted96, and secondly prohibited the envisioned data processing activities to exceed the limits of what is strictly necessary in the light of those purposes.97

93 Digital Rights Ireland, para 33.
95 Digital Rights Ireland, paras 41-44.
96 Digital Rights Ireland, para 49. However, it has, rightfully, been criticized that the CJEU does not genuinely examine the appropriateness of data retention as a tool to fight serious crime: Orla Lynsky, ‘DRI, the Good, the Bad and the Ugly’.
97 Digital Rights Ireland, para 46.
Indeed, the CJEU found that an interference *in casu* could only be accepted if it was ‘*strictly necessary*’ given the combination of the fundamental rights at stake and the seriousness of the found interference.\(^{98}\) However, the CJEU ruled that this last primordial condition was not fulfilled.\(^{99}\) It highlighted that the Directive, in order to reduce the interference to what is strictly necessary, had to lay down clear and precise rules governing the scope and application of the data processing practises on the one hand, and should have introduced a number of safeguards on the other. The EU legislator failed however on both counts.\(^{100}\)

50. More specifically, the Court pointed to the lack of limitations of the data processing in three instances. Firstly, with regard to the initial phase of data collection and retention, it reproached the Data Retention Directive to target *- in a generalised manner -* all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception in the light of the objectives.\(^{101}\) In this view, the Court unequivocally condemned the absence of any link between the data of which the retention is prescribed and the threat to public security that must be countered, to clearly exceed the limits of what is strictly necessary. The CJEU consequently ruled that the retained data should, on the other hand, be limited to (i) data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved in a serious crime, or to (ii) persons whose data could, for other reasons, contribute to the prevention, detection or prosecution of serious offences.\(^{102}\)

Secondly, also pertaining to the following phase of access to the gathered data, the Court considered the Data Retention Directive to have failed in laying down *sufficient objective substantive and procedural criteria* ensuring that the number of persons authorized to access, and make subsequent use of, the collected data was limited to what was strictly needed for the purposes of the preventing, detecting or prosecuting serious offences.\(^{103}\) In particular the fact that such access was not made dependent on the prior review carried out by a court or independent administrative body was disapproved of.\(^{104}\)

Thirdly, the Court finally deemed the data retention period foreseen by the Directive to exceed the limits of what was strictly necessary as well, since it imposed a period between six and twenty-four

\(^{98}\) *Digital Rights Ireland*, para 48. The objective of fighting, even serious, crime such as against terrorism, is not by itself sufficient to pass the *strict necessity* test: *Digital Rights Ireland*, para 51.

\(^{99}\) *Digital Rights Ireland*, para 65.

\(^{100}\) *Digital Rights Ireland*, para 54.

\(^{101}\) *Digital Rights Ireland*, paras 56-57.

\(^{102}\) In this view, the CJEU explicitly disregarded the fact that the retention obligation even applied towards persons for whom there is no evidence capable of suggesting that their conduct might have any link with serious crime: *Digital Rights Ireland*, paras 58-59.

\(^{103}\) *Digital Rights Ireland*, paras 60-61.

\(^{104}\) *Digital Rights Ireland*, para 62.
months, again without any differentiation in the light of the persons concerned or the possible usefulness of the data in relation to the objective pursued.105

51. As indicated, the Court additionally reproached the EU legislator not to have provided the Directive with a sufficient level of safeguards to ensure effective protection of the personal data against the risk of abuse and unlawful access to and use of the data.106 Along these lines, the CJEU primarily criticized the absence of a provision requiring the data to be retained within the EU. Therefore, effective control of compliance with the requirements of data protection and security by an independent authority could, according to the Court, not be ensured.107

52. Having established that the data processing activities imposed by the Data Retention Directive caused an unjustifiable interference with the fundamental rights to privacy and data protection108, the CJEU consequently declared the Directive invalid. However, in light of the presented dissertation, it is moreover the general acknowledgement of the danger caused by large-scaled data processing operations that is of great importance, together of course with the indicated data protection conditions, principles and other insights set out by the CJEU to counter those risks.109

2. Tele2 Sverige AB and Watson and Others

53. In the Tele2 Sverige judgement110, the CJEU ruled a second landmark judgement that built upon the previous discussed case and elucidated certain principles established therein. Primarily, the Court reiterated and stressed the incompatibility of generalised and indiscriminate surveillance with EU data protection law.111 However, it also acknowledged that some circumstances necessitate the retention of –targeted– data and used the Tele2 Sverige judgement to set out the specific circumstances in and conditions under which such data retention activities are allowed.

(1) Facts of the case

54. In the wake of the “Digital Rights Ireland” judgement, both Sweden and the United Kingdom referred to the CJEU for a preliminary ruling, addressing certain national provisions that were adopted on the basis of the invalidated Data Retention Directive and encompassed general and

105 Digital Rights Ireland, paras 63-64.
107 Digital Rights Ireland, para. 68.
108 Digital Rights Ireland, para. 69; Xavier Tracol, ‘CJEU invalidated the data retention directive’, 737.
109 See also: Orla Lynsky, ‘DRI, the Good, the Bad and the Ugly’.
110 Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others [2016] ECLI:EU:C:2016:970 [“Tele2 Sverige AB”].
111 Tele2 Sverige AB, paras 46 and 112.
indiscriminate data retention obligations, combined with broad access possibilities to the collected data. Hence, again the compatibility of the concerned provisions with EU data protection law was questioned.

(2) Ruling of the Court

55. The first part of the Court’s reasoning was quite similar to that in Digital Rights Ireland. The Court ruled that the concerned data processing activities constituted a *particular serious* interference with the fundamental rights enshrined in Articles 7 and 8 of the EU Charter\(^\text{112}\) and subsequently assessed whether such an interference could be justified in the light of the above explained derogation clause embodied in Article 52(1) of the EU Charter.\(^\text{113}\) The focal point of this assessment again boiled down to the question whether the data processing was limited to what was *strictly*\(^\text{114}\) necessary to achieve the – legitimate\(^\text{115}\) – purposes of fighting serious crime, both with respect to the initial phase of data retention and the following phase of access to the collected data.\(^\text{116}\)

56. As far as the envisioned retention of personal data concerns, it came as no surprise that the CJEU declared the provisions at issue problematic. It, once again, provided the clear-cut statement that legislation which prescribes a *general and indiscriminate retention of data* – hence without requiring any relationship between the data to retain and a threat to public security –\(^\text{117}\) exceeds the limits of what is strictly necessary.\(^\text{118}\)

However, thereupon the Court went beyond its prior judgement in Digital Rights Ireland and set out certain specifications under which, on the contrary, the processing of certain personal data is accepted in the light of the Union’s data protection regulation. In this regard, the Court made the elucidation that Articles 7, 8 and 52(1) of the EU Charter, do not preclude the retention of personal data where such encounters clear limits with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted.\(^\text{119}\) In order to ensure this, the CJEU again explicitly required the legislation at stake to both lay down clear and precise rules governing the scope and application of the data retention measure concerned, and

\(^{112}\) Tele2 Sverige AB, paras 99-100.  
\(^{113}\) Tele2 Sverige AB, para 94.  
\(^{114}\) Tele2 Sverige AB, para 96.  
\(^{115}\) Tele2 Sverige AB, para 102.  
\(^{116}\) Tele2 Sverige AB, para 103.  
\(^{117}\) Tele2 Sverige AB, para 106.  
\(^{118}\) Tele2 Sverige AB, para 107.  
\(^{119}\) Tele2 Sverige AB, para 108.
to provide for sufficient safeguards ascertaining the effective protection of data subjects against risks of misuse.\textsuperscript{120}

The main novelties in – and merits of – the \textit{Tele2 Sverige judgement} in this regard firstly relate to the clarification of the CJEU that \textit{objective and well-evidenced criteria} must be used to base the required limitations on\textsuperscript{121}, and that secondly the selected criteria must, most importantly, enable the \textit{identification of persons} whose data is likely to reveal a required link (even an indirect one) with the targeted criminal offences and to contribute to the fight against these crimes, or to the prevention thereof.\textsuperscript{122} Hence, whilst the CJEU in its previous \textit{Digital Rights Ireland ruling} still left the door open for data retention which would not be targeted in terms of the “persons affected” (by choosing the wording “and/or”), the CJEU now made clear that \textit{EU data protection law} only accepts the retention of personal data which is \textit{simultaneously} targeted as to (i) the categories of data; (ii) the means of communication affected; (iii) the retention period adopted and, primarily, (iv) the persons concerned.\textsuperscript{123}

57. The second part of the CJEU’s judgement in \textit{Tele2 Sverige} subsequently focussed on the following phase of access to retained data and on the conditions and safeguards with which the EU and national legislators have to endow the concerned provisions in order to also limit granted access to what is strictly necessary. In this regard, the Court again delivered both repetitive and innovative considerations.

Again the CJEU started off with the unequivocally elucidation that \textit{general access} to all retained data cannot be regarded as limited to what is strictly necessary. Accordingly, also measure regarding access to data must lay down clear and precise binding rules, based on objective criteria, indicating in what specific circumstances and under which conditions access to the personal data can be granted.\textsuperscript{124} Yet again, there must be a genuine link between the accessibility of the retained data and the expressed objectives of fighting serious crime, in particular with respect to the individuals whose data is being disclosed. In this regard, the Court more specifically mandated that access can only be granted to the data of individuals (i) who are suspected of planning, committing, or being implicated

\begin{itemize}
  \item \textsuperscript{120} \textit{Tele2 Sverige AB}, para 109.
  \item \textsuperscript{122} \textit{Tele2 Sverige AB}, para 111.
  \item \textsuperscript{123} Gert Vermeulen, ‘Selective data retention’ (Workshop ‘Targeted surveillance and selective data retention’ International Intelligence Oversight Forum (IIOF2017) The Road Ahead: Dilemmas and Best Practices in Democratic Intelligence Oversight’ Brussels, 21 November 2017), 3-4 (‘Gert Vermeulen, ’Selective data retention’).
  \item \textsuperscript{124} \textit{Tele2 Sverige AB}, para 117.
\end{itemize}
in a serious crime\textsuperscript{125} or (ii) regarding whom there is objective evidence suggesting that their data might contribute to combating such crimes.\textsuperscript{126}

Moreover, the CJEU stressed the necessity of also safeguarding the access to retained personal data with additional substantive and procedural conditions\textsuperscript{127}, and listed in that regard four safeguards that it considers indispensable. Firstly, the Court took the position that access to retained data should be subject to a prior review carried out either by a court or by an independent administrative body. The only possible exception to this general rule may take into account cases of validly established urgency.\textsuperscript{128} Secondly, the competent national authorities to whom access to retained data has been granted must notify the data subjects concerned of their approved access, at least as soon as such notification is no longer liable to jeopardise the investigations proceeded by those authorities.\textsuperscript{129} Thirdly, the Court mandated that the personal data at issue must be retained within the EU. Finally, it also advocated for the irreversible destruction of the data at the end of the retention period.\textsuperscript{130}

\textbf{58.} As in the present case the challenged national legislations failed to fulfil the principles and conditions discussed above, the CJEU denied their compatibility with the EU Charter.\textsuperscript{131}

\textbf{59.} Accordingly, again the CJEU showed to be anything but reluctant to subject issued legislation to a close investigation pertaining to its compliance with EU data protection law, and to establish and further develop certain data protection principles in this process. It must be clear that these indicated principles subsequently all became vital elements of the Union’s data protection framework, in the light of which the presented dissertation will examine the draft 5\textsuperscript{th} AML Directive (Chapter 2).

\textbf{3. PNR Canada (Opinion 1/15)}

\textbf{60.} The last leading case that must be discussed in the light of this thesis, encompasses an opinion that the Court recently delivered pertaining to the agreement concluded between the EU and Canada on the transfer of Passenger Name Record data (PNR data). The Court used this opinion to

---

\textsuperscript{125} \textit{Tele2 Sverige AB}, para 119.
\textsuperscript{126} Where for example vital national security, defence or public security interests are threatened by terrorist activities: \textit{Tele2 Sverige AB}, para 119.
\textsuperscript{127} \textit{Tele2 Sverige AB}, para 118.
\textsuperscript{128} \textit{Tele2 Sverige AB}, para 120.
\textsuperscript{129} \textit{Tele2 Sverige AB}, para 121.
\textsuperscript{130} \textit{Tele2 Sverige AB}, para 122.
\textsuperscript{131} \textit{Tele2 Sverige AB}, paras 112 and 125.
once more establish a considerable number of data protection conditions and principles with which both the national and the EU legislator have to comply.

(1) Facts of the case

61. In 2014, the EU and Canada signed an agreement allowing and governing the systematic transfer, retention, storage and usage of PNR data originating from all air passengers travelling from the EU to Canada, in the advantage of the Canadian competent authorities. However, when the EU Council sought the EU Parliament’s approval, the latter asked for the CJEU’s position towards the compatibility of the PNR agreement with EU law and, in particular, with the fundamental rights to private life and the protection of personal data (Articles 7 and 8 of the EU Charter). Consequently, the Court issued the concerned opinion on the 26th of July 2017, in which it unambiguously denied such compatibility.

(2) Ruling of the Court

62. As the PNR agreement targeted a wide range of personal information, even including sensitive data, it was in the light of the Court’s previous case law no surprise that the CJEU considered the agreement to constitute a clear interference with both the fundamental rights to respect for private life and the protection of personal data. Moreover, it was neither surprising that in the subsequent examination of a possible justification for these interferences, the Court found several difficulties hindering such as well.

63. In essence, the deficiencies in the light of EU data protection law that were indicated by the CJEU relate to four distinct phases of the data processing concerned, and can accordingly be divided as such: (i) the phase of transfer of PNR data to Canada; (ii) the phase of access to and use of the transferred PNR data, prior to air passengers’ arrival to, and upon their departure from, Canadian territory, for profiling reasons; (iii) the phase of access to and use of the transferred PNR data for other reasons, during the data subjects’ stay (iv) the phase of access and use of the PNR data after the data subject has left this territory. The CJEU examined the ‘strict necessity’ of the data processing conducted in all of these phases.

---

132 TFEU, 218(11).
133 Opinion 1/15, paras 124-125.
134 Opinion 1/15, para 126.
135 However, some authors rightfully questioned the appropriateness of the PNR Agreement, as statistics showed that the transfer and use of PNR data were only relevant in a very low number of cases, which contrasts greatly with the high number of travellers whose data was collected and transferred: Elif Mendos Kuskonmaz, ‘Following the digital footprints of
64. With regard to the phase of (collection and) transfer of the PNR data, the CJEU in first instance expressed its concerns pertaining to the categories of data that were targeted by the PNR agreement. On the one hand it found that certain provisions of the PNR agreement were not delineated in a sufficiently clear and precise manner, and on the other, the CJEU also criticized the envisioned transfers of sensitive data (revealing one’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership’ and a person’s health or sex life). The Court stressed that, concerning sensitive data, the pure premise of their possible relevance for the purpose of combating terrorism and serious transnational crime is by itself not sufficient to justify the interference with Articles 7 and 8 of the EU Charter and that the transfer of sensitive data can only be allowed when such encounters a precise and particularly solid justification, based on other grounds as well.

Additionally, the CJEU scrutinized the purpose(s) for which the PNR data was collected and transferred to Canada, advocating and reiterating that such purposes must be expressed by using sufficiently clear and precise rules. In this regard, the PNR agreement both envisaged the primary objective of ‘preventing, detecting or prosecuting terrorist offences or serious transnational crime’ and other additional purposes, including the protection of vital interests of any individual, ensuring the oversight or accountability of the public administration and complying with subpoenas, warrants, or orders made by a court. Where the Court showed a benevolent and accepting attitude towards the first quoted objectives of fighting terrorism and serious crime, and protecting vital interests, it considered the wording of the last two expressed purposes to be “too vague and general” to meet the requirements as to clarity and precision required.

Of great importance is that the CJEU further again expressed its requirements and protection standards as to the provisions governing the ‘public affected’ by the data processing activities allowed for by the PNR agreement. With regard to the first phase of transferring passengers’ PNR data to competent Canadian Authorities, these conditions seem to have taken some distance from those set out in the CJEU’s previous case law, where the processing of personal data was only allowed when such clearly targeted certain data subjects linked, or contributing to the fight against serious crimes (see no.50-56). In its Opinion 1/15 the Court ruled, on the contrary, that the

---

136 Opinion 1/15, para 155.
137 Opinion 1/15, para 165.
138 This entails a clear reference to: EU Charter, Art. 8(2) and GDPR, Art. 5(1)(b).
139 Opinion 1/15, paras 178 and 180.
140 Opinion 1/15, para 181.
envisaged transfer of PNR data of all air passengers to Canada did not exceed the limits of what is strictly necessary.\textsuperscript{141} Hence, even the transfer of PNR data collected from passengers regarding whom no objective evidence exists demonstrating their liability to present a risk to the public security in Canada, is, also in the opinion of the CJEU, accepted.\textsuperscript{142}

The Court invoked two arguments to justify this deviation. Next to the observation that Article 13 of the Chicago Convention subjects all air passengers who wish to enter or depart from Canada to border controls which include their identification by means of PNR data\textsuperscript{143}, the CJEU also seems to consider that the necessary link between the public affected by the data processing practices and the pursued objectives appears later, following the system of automated processing to which the data are subsequently subjected.\textsuperscript{144} Indeed, the envisioned system of ‘profiling’ applied to the data collected in bulk aimed to identify a risk to public security that – at that time unknown – persons could potentially present, in order to subject (only) those exhibiting such a risk to further examination.\textsuperscript{145}

65. In this respect the Court thus seems to accept – justifiable or not – the fulfilment of the strict necessary-condition\textsuperscript{146} because of the selection that is being performed in the second phase of the concerned processing practices, pertaining to the use of the transferred PNR data for profiling reasons.\textsuperscript{147} Along the same lines, the CJEU moreover observed that the exclusion of certain categories of persons or of certain areas of origin would hinder the intentions of such a system of automated processing.\textsuperscript{148}

For the remainder the CJEU mainly focused, in the context of the said second phase, on scrutinizing this system of automated processing of PNR data, establishing a total of four key principles. Pointing to the unavoidable margin of error\textsuperscript{149}, the Court first of all mandated that only non-discriminatory, specific and reliable pre-established models and criteria may be used in the context of automatic data processing, which are able to generate results that “[only] target individuals who might be

\textsuperscript{141} Opinion 1/15, para 189.
\textsuperscript{142} Opinion 1/15, para 186.
\textsuperscript{143} Opinion 1/15, para 188. This argument suggests, however, that the Court’s Opinion 1/15 must be considered as a product deriving from the particular circumstances of the case.
\textsuperscript{144} Opinion 1/15, para 187. See in this regard: Data Protection and Privacy Under Pressure, 151-153.
\textsuperscript{145} However, some authors do not agree with the quoted reversal of the CJEU: Data Protection and Privacy Under Pressure 165-167.
\textsuperscript{146} EU Charter, Art. 52(1).
\textsuperscript{147} Opinion 1/15, para 197.
\textsuperscript{148} Ibid.
under a ‘reasonable suspicion’ of participation in terrorist offences or serious transnational crime”, hence establishing the required link between the public affected and the pursued objectives.150

For the same reasons, the Court secondly only allowed the PNR data to be crosschecked with other reliable, up to date and limited databases that are used in view of combating terrorism and/or serious transnational crime.151 Thirdly, the Court argued that an individual measure that could adversely affect the air passengers concerned may never be based solely and decisively on the result of automated processing of PNR data, and can only stem from an individual re-examination by non-automated means.152 Lastly, the reliability and topicality of the said pre-established models and criteria should, according to the Court, be covered by the joint review of the implementation of the envisaged agreement and take into account both statistical data and results of international research.153

66. Once the passenger reaches Canadian territory without being withheld on reasons of any suspicion of links with terrorism, and his or her PNR data enter into the quoted third phase of data processing by the competent Canadian authorities, the Court again adopted a strict approach and mandated that the use of transferred PNR data by those authorities, during the data subject’s stay in Canada, is only allowed when justified by new circumstances.154 In order to ensure this, the CJEU fully relied upon its previous judgements and the therein-established principles pertaining to the access to and use of gathered personal data and required (i) clear and precise rules, based on objective and evidenced criteria, that define the precise circumstances and conditions under which the Canadian authorities are authorised to make such additional use of the PNR data; (ii) substantive and procedural conditions and safeguards governing such use in order to counter risks of abuse; and (iii) the establishment of a prior review on the use of the retained PNR data, carried out either by a court or an independent administrative body.155

In general, the Court stressed in its Opinion 1/15 that the access to, and use made of, PNR data by the competent Canadian authorities must always serve, and be limited to, the prevention, detection, or prosecution of the targeted crimes.156 In this respect, it argued as well that there should be a link

150 Opinion 1/15, para 172.
151 Ibid.
152 Opinion 1/15, para 173.
154 Opinion 1/15, para 200. However, an exception has to be made when the data are necessary to revise the models and criteria used for the automated analysis of the PNR data: Opinion 1/15, para 197.
155 Opinion 1/15, para 199.
156 Opinion 1/15, para 192.
157 Again except in cases of validly established urgency Opinion 1/15, para 202.
between the pursued objectives and the, clearly and precisely described\textsuperscript{159} authorities competent to process the transferred PNR data, to the extent that the latter’s functions should be related thereto.\textsuperscript{160}

67. In a last phase of PNR data processing, starting with the air passengers’ departure from Canada, the Court has (rightfully) considered that the continued storage of their PNR data is no longer allowed\textsuperscript{161}, unless objective evidence can be brought forward demonstrating that “\textit{a particular passenger may present a risk in terms of the fight against terrorism and serious transnational crime, and such even after his or her departure from Canada}”.\textsuperscript{162} In those specific cases, the further use should, however, again harbour the safeguards established in the Court’s case law, in order to be limited to what is strictly necessary to achieve the expressed objectives.\textsuperscript{163}

As far as concerns the period for which the PNR data can be retained after the passenger’s departure, the Court held that a five-year retention period was not excessive on the condition that the data were held in Canada and were irreversibly destroyed at the end of the concerned period.\textsuperscript{164}

68. Last, but definitively not least, the CJEU has in its \textit{Opinion 1/15} rightfully criticized the envisioned provisions allowing the disclosure of PNR data to, and thus access by, other government authorities and individuals than the competent Canadian authorities as well. Pertaining to the permission included in the PNR agreement to disclose PNR data to other government authorities, the Court stressed the necessity of compliance with the general conditions governing the use of personal data.\textsuperscript{165} \textit{In casu}, the PNR agreement did not, according to the CJEU, fulfil this requirement.\textsuperscript{166}

With regard to the disclosure of PNR data to individuals, the Court adopted an even stricter position and primarily reproached the open and vague wording of the concerned provisions in the PNR agreement. More specifically, the Court considered the PNR agreement to not sufficiently delimit or define (i) the nature of the information that could be disclosed; (ii) the persons to whom such disclosure could be made; (iii) the use that is to be made of the concerned information\textsuperscript{167}; (iv) the

\textsuperscript{159} \textit{Opinion 1/15}, paras 183-185.
\textsuperscript{160} \textit{Opinion 1/15}, para 184.
\textsuperscript{161} \textit{Opinion 1/15}, paras 205-206.
\textsuperscript{162} \textit{Opinion 1/15}, para 207.
\textsuperscript{163} \textit{Opinion 1/15}, para 208. In the PNR Agreement, the CJEU found this requirement not to be fulfilled: \textit{Opinion 1/15}, para 211.
\textsuperscript{164} \textit{Opinion 1/15}, para 209.
\textsuperscript{165} \textit{Opinion 1/15}, para 212. \textit{Inter alia} subjecting the use of data to a prior review – except for cases of urgency – by a court or an independent administrative body: \textit{Opinion 1/15}, para 202.
\textsuperscript{166} \textit{Opinion 1/15}, para 215.
\textsuperscript{167} \textit{Opinion 1/15}, para 216.
terms ‘legal requirements’, ‘limitations’ and ‘legitimate interests of the individual concerned’; or (v) the purpose of the disclosure to the individual, which does, subsequently, not even have to be linked to combating terrorism and serious transnational crime. Furthermore, the disclosure to individuals is not subject to the authorisation of a judicial authority or an independent administrative body. In this view, the Court consequently considered the provisions concerned to again exceed the limits of what is strictly necessary. In the light of the presented dissertation, the CJEU’s critical position towards the disclosure of personal data to individuals must certainly be borne in mind (see no.124).

69. In view of the above and the therein-demonstrated lack of ‘strict necessity’ jeopardizing several provisions of the EU/Canada deal, the CJEU declared the draft PNR Agreement not to be in compliance with the Union’s data protection legislation. With this negative opinion, it is the fourth time that the CJEU has ruled against arrangements for mandatory retention and further processing of personal data and has, in doing so, once again proved to be stringent when it comes to the protection of its citizens’ personal data and privacy.

Admittedly, the Court initially deviated to some extent from its previous case law by accepting the systematic, general and indiscriminate collection, transfer to and use of PNR data for risk identification reasons, and thus seemed to, at least in theory, legitimize mass surveillance. However, the CJEU thereupon avoided a serious fall-back in terms of data protection, as it both reiterated and introduced a number of strict requirements that made the concrete implementation of mass surveillance difficult to be applied in practice. Moreover, the said acceptance of data collection and transfer in bulk can also be explained pointing to the difference in the nature of the relevant data (PNR data as compared to communications data) and by the specific circumstances of the case (profiling for risk identification reasons as part of Canadian border controls and security checks). Therefore, a different position of the CJEU can, in a different setting, not be ruled out.

Accordingly, overall this judgement needs to be perceived as another victory for individual’s fundamental rights to privacy and data protection, contributing to the establishment of a strong and elaborated EU data protection framework.

168 Opinion 1/15, para 217.
169 Ibid.
170 Digital Rights Ireland, Tele 2 Sverige AB, Schrems, and now Opinion 1/15.
171 Data Protection and Privacy under Pressure, 156.
Conclusion

70. The judgements explained above clearly demonstrate the Court’s perseverance to act as a strong defender of the fundamental rights to privacy and data protection\(^\text{172}\), as it consistently highlights and condemns the risks associated with massive and unnecessary databases of (sometimes sensitive) personal data. Relying on, and inspired by, the principles included in the Data Protection Directive, the CJEU in this respect set out in what circumstances and under which conditions a privacy intrusive measure can be adopted in order to be considered limited to what is ‘strictly necessary’.

In general, the Court claimed that Articles 7 and 8 of the EU Charter prohibit data retention and processing ‘in bulk’, leaving member states only with the possibility to collect and use personal data when such is “targeted”, at least pertaining to the public that may potentially be affected. The same applies to the subsequent, but distinct, phase of access to personal data, meaning that also the general granting of access to collected personal data is inadmissible.\(^\text{173}\) Hence, except for the indicated opening the Court has left with respect to data transferring and further processing of PNR data in bulk, the Union’s data protection legislation requires the demonstration of a clear and pre-established link between the envisioned data processing and its objectives. Moreover, each data processing practice or phase must receive protection by an adequate level of substantive and procedural safeguards, countering risks of abuse.\(^\text{174}\)

However, notwithstanding the reiteration of the said principles every time the CJEU is offered the chance hereto, practise shows that neither the Member States, nor the EU legislator fully takes the discussed data protection standards into account when issuing new legislation. Therefore, this thesis aligns with Joe McNamee (Executive Director of European Digital Rights), who explicitly wondered “how many times the Court needs to be asked the same question before EU Member States [as well as the EU itself] start listening”.\(^\text{175}\)

\(^\text{172}\) EU Charter, Art. 7 and 8.
\(^\text{173}\) Hence, the notion ‘processing of personal data’ under EU data protection law implies both the ‘retention’ or ‘collection’ and the subsequent ‘access’ or ‘use’ of the data: Gert Vermeulen, ‘The Paper Shield’, 7.
Conclusion EU Data Protection Framework

71. The EU disposes of a solid and well-elaborated data protection framework, consisting of, firstly, the fundamental rights to privacy and data protection harboured by the EU Charter (no.8-11); secondly, the data protection principles and standards included in the GDPR (no.13-42); and finally, a handful of crucial landmark cases ruled by the CJEU, interpreting the previous two (no.43-70).

All of these components aim to protect EU data subjects against the blind and reckless processing of their personal data as they introduce a range of evermore strict and precise data protection conditions, principles and safeguards, regulating any such activities. Merely relying upon the need to combat serious crimes such as terrorism, as was often the case until recently, clearly no longer suffices to justify highly intrusive data processing operations. Indeed, to be allowed in the light of the Union’s data protection framework, or in a democratic society in general for that matter\(^\text{176}\), privacy intrusive measures need to demonstrate the upmost respect for all of the quoted EU data protection principles. Hence, a real change of mentality in policy-making is required.

CHAPTER II: COMPATIBILITY OF THE DRAFT FIFTH AML DIRECTIVE WITH THE EU DATA PROTECTION FRAMEWORK

72. A second apparent and legitimate concern with which our current society is faced, addresses the recently increased presence of, and fear for, terrorism. The last years have truly witnessed this phenomenon to conquer a central place in most countries of the world, clearly demanding Europe to join its forces in countering the vicious attacks conducted in this context. Subsequently, the EU institutions have assumed office by undertaking numerous initiatives, one of which being the Commission’s action plan against terrorist financing, announced in February 2016. A fundamental part of this plan envisioned a fifth revision of the AML Directive, which seeks to strengthen the current 4th AML Directive’s transparency rules as regards the real owners of companies and trusts, and by addressing new means of terrorist financing.

However, as the 4th AML Directive already sought to achieve its objectives of fighting terrorism and money laundering by encompassing wide-ranging data processing practises, the question – constituting the subject of the present dissertation – boils down to whether and to what extent the (even more privacy intrusive) draft 5th AML Directive still appears compatible with the EU data protection framework discussed above (Chapter II).

73. In order to provide a deliberated answer to this research question, the first section of the current Chapter will provide an outline of the envisioned draft 5th AML Directive, focussing on the data processing practises imposed within its context (section 1). In a second section, the explained draft Directive will be subjected to a close examination in the light of Union’s data protection framework discussed above (section 2). Finally, a conclusion will be formulated (Conclusion).

Section 1: Outline of the draft 5th AML Directive

74. In order to create a comprehensive impression of the potential impact the 5th AML Directive would have on an individual’s privacy with respect to their personal data, it seems necessary to assess the total package of data processing provisions it would establish, entailing the combination of both current and envisioned rules in that regard. Hence, in the following, a discussion of the

---


179 Also the Article 29 Working Party advocated a ‘holistic approach’ to examine whether envisioned legislation is still proportionate: Article 29 Data Protection Working Party, ‘Opinion 01/2014 on the application of necessity and
draft 5th AML Directive will – to the extent necessary – be presented, respectively addressing its ratio, scope, and substantive provisions. New additions and considerable changes introduced by the draft 5th AML Directive as compared to the currently applicable 4th AML Directive will be indicated.

1. Ratio and envisioned changes

75. In general, the draft 5th AML Directive is, as did its predecessors, designed to improve the tools used to combat both terrorist financing and money laundering acts at EU level, since flows of illicit money are considered to threaten the integrity, stability and reputation of the Union’s financial sector and of the internal market as a whole.\textsuperscript{180} More in particular, the European Commission proposed the fifth revision of the AML Directive on 5 July 2016, as part of its action plan against terrorist financing\textsuperscript{181}, seeking to further eliminate the money smuggling routes made possible by the Union’s financial system by overall increasing the concerned transparency rules and by targeting new means of terrorist financing.\textsuperscript{182}

Of the upmost importance in the context of this dissertation is, however, that the Commission’s proposal not solely entailed a reaction to the horrible surge of terrorist attacks Europe recently had to endure, but was also developed in the wake of the Panama Papers revelations of April 2016.\textsuperscript{183} Therefore, the proposal also intended to boost ‘tax transparency’ and tackle ‘tax abuse’.\textsuperscript{184} Accordingly, the particular changes proposed by the Commission simultaneously served objectives of combating terrorist financing, money laundering and tax evasion.

76. The Commission’s proposal subsequently entered into a phase of negotiations within and between the EU Council and the EU Parliament. After an approving opinion of the European Economic and Social Committee (EESC)\textsuperscript{185} but an opposing one of the EDPS\textsuperscript{186}, the EU ambassadors confirmed in this context, on 20 December 2017, a political agreement reached between the presidency and the European Parliament on “strengthened EU rules to prevent money laundering proportionality concepts and data protection within the law enforcement sector” [2014] WP 211 <http://www.pdpjournals.com/docs/88168.pdf> accessed 3 April 2018.

\textsuperscript{180} 4th AML Directive, Art. 1(1); draft 5th AML Directive, Art. 1(1).

\textsuperscript{181} Commission Action Plan.

\textsuperscript{182} Commission Press release 5th AML Directive.

\textsuperscript{183} Commission, ‘Communication from the Commission to the European Parliament and the Council on further measures to enhance transparency and the fight against tax evasion and avoidance’ (Communication) COM(2016) 451 final, 5.

\textsuperscript{184} Commission Press release 5th AML Directive.


and terrorist financing”. The draft version of the 5th AML Directive that was presented in this regard is recently, on 19 April 2018, adopted in a first plenary reading and has thus entered into the final stage of adoption by the EU Council, which it will, however, withstand as well. The examination carried out in section 2 of this thesis will examine its compatibility with the Union’s data protection framework.

77. The Council’s press release pertaining to the draft 5th AML Directive disclosed four main changes that are to be expected in comparison with the currently applicable 4th AML Directive.

First and foremost, the draft 5th AML Directive aims to enforce more transparency with regard to the ownership of companies and trusts by broadening up the access to beneficial ownership registers in several aspects (see no. 101-103). Secondly, the draft 5th AML Directive focuses on new, low-cost, channels and modalities that are used to transfer illegal funds into the Union’s economy. In this regard, primarily risks occurring by the use of prepaid cards and virtual currencies are addressed (see no. 79). Thirdly, the improvement of the cooperation between the Member States’ FIU’s is planned as well (see no. 103). The fourth and last change, according to the Council at least, concerns the improvement of the control exercised on ‘high-risk third countries’. It is to say, a country’s appearance on the (renewed) list of high-risk third countries will instigate enhanced due diligence measures resulting in closer monitoring (see no. 93-95).

78. However, a fifth substantial change that -especially in the light of the Commission’s initial proposal- seems to be implied in the draft 5th AML Directive, entails its intention of picking up the fight against tax evasion as well. Admittedly, the eventual draft 5th AML Directive proposed by the EU Council and Parliament refrains from explicitly mentioning ‘tax reasons’ as one of its objectives and claims to shift the focus back to the traditional aims of solely fighting terrorist financing and money laundering. However, the tools that were specifically designed by the Commission to achieve the said tax purposes are, albeit in a slightly modified form, preserved and will certainly be used as such (e.g. tax authorities are still given extensive access to information collected for anti-money laundering purposes and the provisions granting public access to beneficial ownership information of companies remained in the text as well, see resp. no. 97 and 101 ). Such raises of course clear

questions with regard to the principles of purpose limitation and proportionality explained above (see no. 129).

2. Scope ratione personae of the AML Directive

79. The range of entities that must obey with the obligations contained in the draft 5th AML Directive [hereinafter: ‘obliged entities’] definitively is to be considered as being broad bearing in mind that the envisaged Directive even further expands the already comprehensive list laid down in the 4th AML Directive. As the listed obliged entities will also provide a useful indicator of the ‘public affected’ by the concerned data processing activities, see no. 118), an examination hereof cannot be left out.

Firstly, the main entities targeted by the draft 5th AML Directive are still the credit and financial institutions.\textsuperscript{190} Indeed, it goes without saying that banks, investment firms, insurance undertakings and their branches and subsidiarity’s are the most important guardians of the well-functioning of the Union’s financial system. The second targeted group subsequently consists of auditors, external accountants, tax advisors and other professionals offering some kind of assistance in tax matters\textsuperscript{191}, as they too are supposed to have access to the required expertise and means to prevent the misuse of the financial sector. Thirdly, the envisaged update of the AML Directive also applies to notaries and other independent legal professionals that, on behalf of their clients, participate in any financial or real estate transaction, or that assist their clients in certain other listed activities dealing with more serious financial transactions.\textsuperscript{192} Along the same lines, also trust and company service providers that are not yet covered by one of the previous categories\textsuperscript{193}, and certain estate agents\textsuperscript{194} are included in the scope \textit{ratione personae} of the draft Directive. Quite staggering is that further even natural or legal professionals trading in \textit{goods} are subject to the draft 5th AML Directive, as soon as made or received payments in cash exceed, by itself or in combination with other linked transactions, an amount of 10 000 EUR\textsuperscript{195} and lastly the presented list of obliged entities is finalized by the inclusion of gambling service providers.\textsuperscript{196}

In addition to these quoted entities that are already subject to the currently applicable 4th AML Directive, and in the light of its ratio mentioned above (see no. 75), the draft 5th AML Directive

\textsuperscript{190} Draft 5th AML Directive, Art. 2(1)(1) and (2).
\textsuperscript{191} Draft 5th AML Directive, Art. 2(1)(3)(a).
\textsuperscript{192} Draft 5th AML Directive, Art. 2(1)(3)(b).
\textsuperscript{193} Draft 5th AML Directive Article 2(1)(3)(c).
\textsuperscript{194} Draft 5th AML Directive Article 2(1)(3)(d). This provision has been expanded in comparison with the 4th AML Directive.
\textsuperscript{195} Draft 5th AML Directive, Art. 2(1)(3)(f).
\textsuperscript{196} Draft 5th AML Directive, Art. 2(1)(3)(f) Directive. However, Member States are allowed to fully or partially exempt these entities when such is justified on the basis of an appropriate risk assessment: draft 5th AML Directive Art. 2(2).
intends to newly introduce several other groups of obliged entities as well. More particularly, virtual and fiat currency exchange platforms, custodian wallet providers and certain individuals active in the world of art works are, according to the draft 5th AML Directive, obliged to apply the Directive and thus the customer due diligence controls as well.

80. Not unimportantly, however, is that the Member States are allowed to extend the scope of the Directive even further to also cover other entities which they consider to engage in ‘risky’ activities in terms of money laundering and terrorist financing, as well as to adopt or retain in force stricter provisions in that regard. Hence, Member States are given a considerable margin of appreciation as to which entities they compel to carry out the data processing practices envisioned by the draft 5th AML Directive.

81. Accordingly, it seems hard to deny the comprehensiveness of the entities that, based on the draft 5th AML Directive, are obliged to engage in data collecting, processing and/or sharing activities. It must be clear, however, that such a wide range of obliged entities equals an, at least, equally wide range of clients whose fundamental rights to respect for privacy and data protection are interfered with.

3. Data processing obligations imposed by the draft 5th AML Directive

82. As indicated, the draft 5th AML Directive imposes an empowered set of obligations on the entities discussed above, of which a considerable part involves the collection, analysis, storage and sharing of personal data. More particularly, the draft Directive requires the obliged entities on the one hand to carry out ‘customer due diligence’ measures (see no. 83-97), and to identify and disclose the beneficial owners of companies, trusts and similar structures on the other (see no. 98-103).

(1) Customer due diligence measures

a. Collection of customer identification data

83. The core of the draft 5th AML Directive is formed by the strengthened ‘customer due diligence measures’, which entail precautionary provisions requiring the obliged entities in certain specified

---

197 Draft 5th AML Directive, Art. 2(1)(g).
198 Draft 5th AML Directive, Art. 2(1)(h).
199 Provided that the value of the transaction, or of a series of linked transactions, amounts to €10,000 or more: draft 5th AML Directive, Art. 2(1)(ha)-(hb)
201 Draft 5th AML Directive, Art. 5.
events to gather and monitor information pertaining to the identity of those involved in financial transactions and/or business relationships, as well as information disclosing the origin, purpose, and overall context of a certain amount of illicit money that one attempts to move through the Union’s financial system.

84. In this regard, it must be noted that the draft 5th AML Directive continues to rely on the risk-based approach introduced by the 4th AML Directive, whereby a higher risk of money laundering or terrorist financing justifies more intrusive procedures and rigorous controls and vice versa. This approach is translated in the establishment of three categories of customer due diligence obligations, entailing firstly a general set of customer due diligence measures, secondly a simplified version of them and lastly certain enhanced measures. However, before discussing these three categories, a brief outline of the scope ratione materiae of the customer due diligence measures will be provided.

a.i. Transactions subjected to customer due diligence measures

85. First of all, credit and financial institutions are bound to carry out customer due diligence measures vis-à-vis both the owners and beneficiaries of accounts, passbooks or safe deposit boxes, before letting their clients make use thereof. Along the same lines, the draft 5th AML Directive requires the collection of customer identification data at the time of establishment of a certain business relationship between any of the obliged entities and their customers.

However, also later on, before executing certain occasional transactions, the obliged entities must gather and scrutinize information concerning the involved parties and features of the concerned transactions. More specifically, due diligence measures have to be carried out in case of occasional transactions amounting to at least 15 000 EUR; transfers of funds that are (at least partially) executed by electronic means through a payment service provider and exceed a threshold of 1 000 EUR; trades in goods when they cross a limit of 10 000 EUR and gambling services pertaining to transactions surmounting 2 000 EUR. Moreover, customer due diligence measures are also required when dealing with transactions encountering some kind of suspicion of money laundering or

---

202 Draft 5th AML Directive, Section 2 “risk assessment”.
203 Draft 5th AML Directive, Art. 10(1).
204 Draft 5th AML Directive, Art. 11(a).
terrorist financing (regardless of any derogation, exemption or threshold) and when the veracity or adequacy of previously obtained customer identification data is questioned.206

86. Accordingly, also the range of transactions inciting the collection and further processing of customer identification data is broadly described, which again causes the ‘public affected’ by these measures to be quite extensive as well.

a.ii. General Customer due diligence information

87. Firstly, the customer due diligence measures imply that the obliged entities must establish and verify the identity of their customers207 and, when applicable, their representatives.208 For these means, all kinds of documents, data or other information originating from reliable and independent sources may be used.

Secondly, also the identity of the beneficial owners (see Annex, (iii)) and their possible representatives209 needs to be, again by means of all reasonable measures, unravelled and verified so that the obliged entity gains full understanding of the person of the beneficial owner, the ownership and control structure of its customer, especially in more complex arrangements such as trusts, companies, foundations and similar legal arrangements.210

In this regard, it must be highlighted that the draft 5th AML Directive newly introduced the obligation for the Member States to put in place centralised automated mechanisms, such as central registries or central electronic data retrieval systems, to store the quoted customer identification data of persons holding or controlling payment and bank accounts, or safe deposit boxes, with a certain credit institution.211 Important may definitely be, however, that Member States are allowed to make “other essential information” accessible through this mechanisms as well.212

Thirdly, when the transactions concern life or other investment-related insurance businesses, the name of the beneficiary must additionally be registered. If the beneficiaries are designated by characteristics, class or other means, the targeted entities must obtain sufficient information to

206 Draft 5th AML Directive, Art. 11(b)-(f).
209 Ibid.
211 Draft 5th AML Directive, Art. 32(a)(1)-(3). Furthermore, also information which allows the identification of any (natural or legal) person owning real estate must be made accessible: draft 5th AML Directive, Art. 32(b)(1).
212 Draft 5th AML Directive, Art. 32(b)(1)
identify the beneficiary at the time of the pay-out. The same applies towards beneficiaries of trusts or similar legal arrangements that are designated by particular characteristics or class.

88. Further, next to the quoted identification obligations, the customer due diligence measures compel the obliged entities to assess and gather information as well on the purpose and intended nature of the business relationship, the aim of which is to ascertain the legitimacy of thereof.

89. Lastly, the draft 5th AML Directive takes an important extra step by also requiring the obliged entities to continuously monitor their business relationships, inter alia, by persisting to scrutinize the transactions undertaken throughout the entire duration thereof.

90. Although obliged entities must carry out each of the quoted customer due diligence measures, they are offered some margin of appreciation to, based on a risk-sensitive assessment, determine the specific extent of those measures. In this respect, the draft Directive (only) mandates that the measures must be appropriate in view of the identified risks of money laundering and terrorist financing. Along the same lines, the draft Directive also requires the obliged entities to apply the customer due diligence measures both towards all new customers and, at appropriate times, towards existing ones. However, which existing customers are targeted is again primarily left to the obliged entities to, inter alia in view of a risk-sensitive basis, decide. Hence, surely enough room is offered to adopt broad interpretations of the said customer due diligence measures.

91. When the obliged entities are unable to comply with the customer due diligence requirements as discussed above, they must restrain from executing the intended transactions or must terminate the business relationship. In those circumstances the entities moreover have to consider reporting the transaction at stake to the Financial Intelligence Units ['FIU’s'] (see Annex, (vii)) as being ‘suspicious’ (see no. 97).

---

217 The listed entities have to take into account the variables set out in Annex I when carrying out this risk assessment: draft 5th AML Directive, Art. 13(3).
221 Ibid.
a.iii.  Simplified customer due diligence information

92. In the light of the indicated risk-based approach adhered by the draft 5th AML Directive, Member States and obliged entities are allowed to prescribe simplified customer due diligence measures where they consider the intended transactions to imply low risks in terms of money laundering or terrorist financing.\(^{223}\) However, such does not release the obliged entities from monitoring and checking the concerned business relationship for unusual or suspicious transactions.\(^{224}\)

a.iv.  Enhanced customer due diligence information

93. On the contrary, the draft 5th AML Directive compels the obliged entities to apply enhanced customer due diligence measures in case of an increased risk of money laundering or terrorist financing. In this regard, the draft Directive explicitly lists three types of situations that are deemed to imply such higher risks on the one hand, and leaves room for the Member States and obliged entities to additionally establish “other high-risks cases” on the other.\(^{225}\)

First of all the draft Directive requires enhanced measures when obliged entities are confronted with transactions that are complex, unusual or unusually large, or with transactions that lack an apparent economic or lawful purpose.\(^{226}\) Secondly, the enhanced measures must be applied to business relationships or transactions that in some way involve high-risk third countries\(^{227}\) and lastly also political engagement elicits an increased level of data collection and monitoring obligations, as “politically exposed persons” (Annex, (iv)) -together with their entire families and close associates (Annex, (v) and (vi))- are specifically targeted by the draft 5th AML Directive as well.\(^{228}\) In this regard, the obliged entities are requested to have in place appropriate risk management systems to determine whether the customer, its beneficial owner or concerned beneficiaries are politically exposed persons.\(^{229}\)

\(^{223}\) Draft 5th AML Directive, Art. 15(1).
\(^{224}\) Draft 5th AML Directive, Art. 15(3).
\(^{225}\) Draft 5th AML Directive, Art. 18a-24. When assessing the risks of money laundering and terrorist financing, Member States and obliged entities must take into account at least the factors of potentially higher-risk situations set out in Annex III: draft 5th AML Directive, Art. 18(3).
\(^{226}\) Draft 5th AML Directive, Art. 18(2).
\(^{227}\) Draft 5th AML Directive, Art. 18a(1) and 19(1).
\(^{228}\) Draft 5th AML Directive, Art. 20-23. The draft 5th AML Directive introduces the obligation for the Commission to issue a list of all prominent public functions in the sense of Article 3(9), which encompasses a description of ‘politically exposed persons’, based on the thereto issued lists of both the Member States and international organisations (Article 20a(3) draft 5th AML Directive).
\(^{229}\) Draft 5th AML Directive, Art. 20(a) and 21.
94. The particularly required ancillary measures demand, *inter alia*, to examine the background and source of concerned business relationships, transactions and funds\(^{230}\), to examine their purpose and nature\(^{231}\), to obtain additional information on the (wealth of) customers and their beneficial owner(s)\(^{232}\) and to generally increase the degree and nature of their monitoring\(^{233}\) and subsequent reporting.\(^{234}\) In some of the quoted circumstances the establishment or continuation of a certain business relationship or transaction is even hindered or prohibited\(^{235}\), or necessitates the approval of the senior management.\(^{236}\)

95. In terms of personal data processing, the enhanced due diligence measures imply that certain individuals, that are considered ‘risky’, are *extra targeted* in such a way that additional (personal) data are being collected (and further processed) and that closer monitoring is being conducted as compared to other individuals or legal entities who do not dispose of a ‘high-risk-profile’. Once again, it must be noted in this regard that the Member States, and notably the obliged entities themselves, have a considerable say in designating the groups or situations that encounter more privacy intrusive measures.\(^{237}\) The general and individual risk assessments that obliged entities in that view must perform can, moreover, be considered as a certain form of ‘profiling’ of their (natural) clients within the meaning of Article 4(4) GDPR (Annex, (vii)).\(^{238}\) Along the same lines, the quoted systems that obliged entities must have in place to uncover whether a certain individual is to be considered a “politically exposed person”, can be perceived as encompassing the gathering and processing of sensitive data within the meaning of Article 9(1) GDPR (Annex, (iii)).

*b. Retention of the customer identification data*

96. Another important aspect in the light of data protection relates to the obligation for the obliged entities to *retain* the collected customer identification data for a certain period as well. More specifically, a copy of the documents drafted to comply with the customer due diligence measures, as well as of the supporting evidence and *records of the transactions*, must be stored for a period of maximum five years after the end of the concerned business relationship or transaction.\(^{239}\) 

---

\(^{230}\) Draft 5th AML Directive, Art. 18a(1)(c); 18(2) and 20(b)(ii).

\(^{231}\) Draft 5th AML Directive, Art. 18a(1)(b) and (d),18(2) and

\(^{232}\) Draft 5th AML Directive, Art. 18a(1)(a)-(c).

\(^{233}\) Draft 5th AML Directive, Art. 18a(1)(f); 18(2) and Article 20(b)(iii).

\(^{234}\) Draft 5th AML Directive, Art. 18a(2)(b).

\(^{235}\) Draft 5th AML Directive, Art. 18(a)(2)(c)-(3).

\(^{236}\) Draft 5th AML Directive, Art. 18a(1)(e); 19 and 20(b)(i).

\(^{237}\) Draft 5th AML Directive, Art. 18(1).


\(^{239}\) Draft 5th AML Directive, Art. 40(1)(a)-(b).
States may however, on the basis of their risk-assessment, prescribe further retention up to an additional period of again five years. Upon expiry of this retention period, the personal data concerned must be deleted.

c. Access to and disclosure of the customer identification data

97. When any of the obliged entities know, suspect or have reasonable grounds to suspect that certain funds are related to terrorist financing or proceeded from criminal activity, they must notify the suspicious transaction to the FIU’s of their Member State. In this context, the obliged entities must substantiate such notification with the information they obtained by carrying out the quoted customer due diligence measures and must thus disclose the concerned customer identification data. Furthermore, the FIU’s have the right to request the obliged entities for specific (additional) information pertaining to certain clients or transactions as well, and to access the central registries or systems indicated in paragraph 87 by themselves.

Thereupon, it is up to the FIU to analyse the notifications and to, where they indeed consider the notification grounded, on their turn, disseminate the results thereof to the competent authorities (Annex, (viii)) so these can take appropriate action. Again, a competent authority may, however, on its own ask the obliged entities and FIU’s to disclose certain gathered customer due diligence data, and has full access to the quoted central registers by itself. In this regard it seems appropriate to highlight that also authorities with other competences than those of preventing and detecting money laundering and terrorist financing offences, such as tax authorities, are designated as ‘competent authorities’ within the meaning of the draft 5th AML Directive (Annex, (viii)).

The FIU’s should respond to requests for information by competent authorities when those are motivated by concerns relating to money laundering, associated predicate offences or terrorist financing and provided that such would neither have a negative impact on ongoing investigations, nor would be clearly disproportionate in light of the legitimate interests of the person concerned.

---

240 Draft 5th AML Directive, Art. 40, in fine. In that case, the national law should determine under which circumstances obliged entities may or shall retain the concerned data for the additional period of five years.
241 Ibid.
242 Draft 5th AML Directive, Art. 33(1)(a). However, there exist two exemptions to this rule: draft 5th AML Directive, Art. 34.
244 Draft 5th AML Directive, Art. 32(3) and (8).
245 Draft 5th AML Directive, Art. 32a(2).
246 Draft 5th AML Directive, Art. 32(8).
247 Draft 5th AML Directive, Art. 32(3).
249 Draft 5th AML Directive, Art. 32a(2).
251 Draft 5th AML Directive 32(5).
(2) Beneficial ownership information

a. Collection of beneficial ownership data

98. A second highly important set of information gathering and processing obligations targets to serve the overall goal of combatting terrorist financing and money laundering by obtaining complete insight in the real ownership of companies, trusts and similar structures active within the Union’s financial sector.

In this regard, corporations and all other legal entities must obtain and hold “adequate, accurate and current information on their beneficial ownership”, which they subsequently have to share with the obliged entities during the carrying out of the due diligence measures discussed above.252 The draft 5th AML Directive explicitly clarifies hereby that such implies the disclosure of information pertaining to the shares, voting rights, ownership interests and other means of control of the beneficial owner(s) of those entities, as well as their full names, months and years of birth, nationalities and countries of residence.253 The same obligations apply, moreover, to trusts and other similar legal arrangements, where particularly the identity of the settlor, trustee(s), protector, (class of) beneficiaries and of any other natural person exercising the “ultimate control” over the trust must be shared as well.254

99. A key change that in that regard is introduced by the 4th AML Directive, and is preserved by the draft 5th AML Directive, is the creation in each Member State of central registers of ultimate beneficial owners [hereinafter: ‘UBO’s’], in which the beneficial ownership data discussed above must be stored.255

b. Retention of the beneficial ownership data

100. The beneficial ownership information must, in first instance, be retained within the said UBO’s during the entire life of the concerned entities and must, thereafter, be retained within the national registers and the system of interconnection of registers for an additional period between five and ten years after the company, trust or similar arrangement has been struck off from their registers.256

252 Draft 5th AML Directive, Art. 30(1).
253 Draft 5th AML Directive, Art. 30(5)(2) and 31(4)(1).
254 Draft 5th AML Directive, Art. 31(1)-(2). The draft 5th AML Directive specifies that Member States must identify the characteristics to determine where legal arrangements have a structure or functions similar to trusts with regard to such legal arrangements governed under their law: draft 5th AML Directive, Art. 31(1) and 31(10).
255 Draft 5th AML Directive, Art. 30(3) and 31(3a).
256 Draft 5th AML Directive, Art. 30(10) in fine and 31(9) in fine.
c. Access to and disclosure of the beneficial ownership data

101. A broad range of actors is, to say the least, subsequently offered access to the said beneficial ownership information. Indeed, the accessibility of the concerned data was already broadly described in the 4th AML Directive and is even further extended within the context of the draft 5th AML Directive. Hence, the latter Directive intends to make the beneficial ownership data, both with regard to companies and trusts, and regardless of the risk they present, accessible to three main categories. First of all, an absolute right of access to the beneficial ownership register is again given to the competent authorities and FIU’s. Secondly, also obliged entities that intend to carry out (additional) customer due diligence measures have a right of access and finally, even “any member of the general public” may access the (personal) data concerned. However, with regard to this latter category a distinction is being made between the access to the beneficial ownership information of companies, which is completely open to the public without imposing any additional preconditions, and such access vis-à-vis trusts and similar structures, where at least the demonstration of a “legitimate interest” is required to provide some kind of safeguard towards the concerned data. On the other hand, Member States may however allow for a wider access with respect to these latter entities as well, and may thus lose the said safeguard after all.

102. Hence, the Directive went very far in realizing its aim to increase transparency with respect to the beneficial owners of all companies, trusts and similar structures, to a level where the comprehensiveness of the accessibility of the quoted beneficial ownership data can, notwithstanding its privacy intrusive character, not be disregarded (see no. 123-127). Admittedly, certain counterbalance is provided to the extent that an exemption can, on a case-by-case basis, be made where access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail,
violence or intimidation, or where the beneficial owner is a minor or otherwise incapable.\textsuperscript{264} However, one could question why the exception has been drawn up in such a narrow fashion.

\textbf{103.} Lastly, it must be noticed that another innovation envisaged by the draft 5\textsuperscript{th} AML Directive introduces a high level of interconnection between the UBO’s of the different Member States.\textsuperscript{265} However, a discussion thereof would exceed the limits of this dissertation.

\textbf{Conclusion}

\textbf{104.} It must be clear that the overall stricter approach envisioned by the draft 5\textsuperscript{th} AML Directive increases and supplements the severe data processing obligations that were already implied in the 4\textsuperscript{th} AML Directive\textsuperscript{266} and introduces by doing so a notable ensemble of privacy intrusive measures that need to be abided by the obliged entities. In order to meet those requirements, and to safeguard themselves from any penalties prescribed in the draft Directive, obliged entities will most likely be inclined to gather, retain and disclose wide lists of information precisely identifying the individuals involved in business relationships or transactions, the specificities of such relationships or transactions, political interests involved and beneficial owners concerned. Moreover, the said entities might consider the installation or upgrade of screening tools, or the development of data mining systems, to comply with their obligations to monitor and detect any suspicious activity conducted under their watch.\textsuperscript{267}

In this view, it appears crucial to examine the said amendments from a data protection perspective and assess whether, and to what extent, the agreed draft 5\textsuperscript{th} AML Directive can be considered justified in the light of the Union’s data protection framework. Indeed, any privacy intrusive practise, even designed for utmost legitimate purposes, such as countering terrorist financing, must be in line

\textsuperscript{264} Draft 5\textsuperscript{th} AML Directive, Art. 30(9) and 31(7a).
\hfill \textsuperscript{265} Draft AML Directive, Art. 30(10) and 31(9).
\hfill \textsuperscript{267} In this regard, the European legislator has, rightfully, been criticized for forcing the obliged entities to “throw data protection principles out of the window” in order to meet the severe expectations withheld to fight terrorist financing and money laundering: Camilleri Preziosi, ‘Finding the balance between data protection and AML requirements’ (Lexology, 23 June 2017) <https://www.lexology.com/library/detail.aspx?g=8aabf8f8-33c1-456d-869b-ef1f56ec0e8> accessed 7 April 2018.
with the legislative standards of the EU on the right to privacy in relation with one’s personal data (Chapter I).\textsuperscript{268}

\textbf{Section 2: Assessment of the draft 5\textsuperscript{th} AML Directive in the light of the EU data protection framework}

\textbf{105.} In the current section, the compliance of the draft 5\textsuperscript{th} AML Directive with the Union’s data protection framework, as presented above (Chapter II), will be subjected to a thorough investigation. Hereto, the method of analysis traditionally applied by the CJEU will be followed.

\textbf{1. Interference with the fundamental rights to privacy and data protection}

\textbf{106.} It only needs a mere reference to the CJEU’s case law discussed above to know that the data processing obligations enshrined in the draft 5\textsuperscript{th} AML Directive give rise to a clear interference with both the fundamental rights to respect for private life and to data protection harboured by the EU Charter (Articles 7 and 8). Indeed, multiple provisions of the draft Directive provide for the processing of information relating to an identified or identifiable individual, which is according to the CJEU sufficient to cause the said interference with both fundamental rights (see no. 47, 55 and 62). This is, moreover, true with respect to both the initial phases of data collection and retention, as well as with regard to the subsequent phases of access to, and use of, the retained data.

\textbf{2. Justification of the found interference}

\textbf{107.} When an interference with the Union’s fundamental rights is found, the (only) next step to do is to examine whether such interference can be justified in the light of Article 52(1) of the EU Charter. As explained above, this provision only allows restrictions that (i) are provided for by law; (ii) respect the essence of the fundamental rights concerned and (iii) are proportional and necessary to (iv) serve certain legitimate objectives. Accordingly, in the following the fulfilment of those conditions by the draft 5\textsuperscript{th} AML Directive will be investigated. Hereby, the focal point will, \textit{what did you expect}, lie on the question of proportionality and necessity of the envisioned data processing in the light of its pursued objectives of countering terrorist financing and money laundering.

\textsuperscript{268} Data Protection and Privacy under pressure, 147; Cian C Murphy, \textit{The EU Counter-Terrorism Law: Pre-Emption and the rule of Law} (Hart Publishing 2015) 149-150.
(1) **Legal basis**

108. The first condition is evidently fulfilled as the draft 5th AML Directive will, at least when it is fully adopted by both the EU Parliament and Council, serve as a sufficiently clear legal basis for the data processing activities provided within its context. In this view, data processing conducted on the basis of the draft Directive must also be considered ‘lawful’ within the meaning of Article 6(1)(c) GDPR, which, in relation to the first key data protection principle, allows processing that is necessary for compliance with a legal obligation to which the controller is subject (see no. 25).

(2) **Respect the essence of the fundamental rights and freedoms**

109. Secondly, it seems highly unlikely that the CJEU would consider the data processing practices provided for by the draft 5th AML Directive to as such adversely affect the essence of the quoted fundamental rights. Indeed, the draft Directive explicitly declares Articles 7 and 8 of the EU Charter, as well as Directive 95/46/EC and Decision 2008/977/JHA fully applicable to any data processing conducted within its limitations. In addition to that, the draft Directive also contains a number of provisions expressing the necessity to respect the Union’s data processing rules and preserves several references to specific (aspects of) the quoted data protection principles. Hence, claiming that the fundamental rights are completely and essentially disregarded would be too far-reaching.

(3) **Serving objectives of general interest**

110. The CJEU repeatedly elucidated, amongst others in its judgements explained above, that objectives of fighting international terrorism and serious crime, such as pursued by the draft 5th AML Directive, genuinely constitute objectives of general interest (see no. 48, 55 and 62). Hence, also the third condition is fulfilled.

(4) **The principle of proportionality**

111. Most importantly, however, the data processing provisions envisioned by the draft 5th AML Directive must be proportional in the light of its pursued objectives of countering terrorist financing and money laundering in order to be justifiable in the light of the fundamental right to privacy in relation to personal data, as well as in the light of the data minimization principle contained within

---

271 Draft 5th AML Directive, *inter alia*, Art. 7; 8(2); 30(1)(4)(5); 31(1)(4)(9); 40(1);41 and rec. 3; 20; 21a; 22a; 26; 29; 30 and 40.
the GDPR (see no. 33). As continuously clarified in the CJEU’s case law, such means that the data processing concerned must, on the one hand, be appropriate to attain the said objectives and, on the other, may not exceed the limits of what is necessary to achieve these purposes (see no. 49).

a. Appropriateness of the data processing

112. With regard to this first component of the proportionality principle, it can be noticed that, almost as a general rule, the CJEU does not pay too much attention to the question whether or not a found interference is appropriate, but immediately moves on to the question whether such interference is necessary to reach the expressed objectives. Although such an approach can certainly be criticized – the CJEU should demand for specific evidence, including figures and statistical material demonstrating (assumed) results of the processing measures –, it leads to the assumption that the Court would also accept the appropriateness of the draft 5th AML Directive in the light of its pursued objectives.

b. Strict necessity of the data processing

113. Given its importance, a considerable part of this dissertation will be devoted to assessing whether the draft 5th AML Directive is limited to what is (strictly) necessary to achieve its purposes of preventing terrorist financing and money laundering. As the quoted necessity test must be withstood in both the initial phases of data collection and retention, as well as within the subsequent phases of access to, and use of, the gathered data (see no. 50, 56-57, 63 and 70), a division between both phases will be upheld.

b.i. Collection and retention of personal data provided for by the draft 5th AML Directive

114. It is clear from the judgements explained above that the strict necessity condition primarily prohibits any general and indiscriminate collection and retention of personal data, and only leaves room for data processing which is simultaneously “targeted” with respect to the (i) categories of data to be retained; (ii) the means of communication affected; (iii) the adopted retention period and, most importantly, (iv) the data subjects. Hence, in each of those aspects a clear link with the pursued objectives must be demonstrated (see no. 56). To ensure this, the CJEU explicitly required national legislation to, on the one hand, lay down clear and precise rules that, on the basis of objective and well-evidenced criteria, indicate in what circumstances and under which conditions

---

272 Digital Rights Ireland, para. 48 and 52.
data may be collected and retained, and to, on the other, establish sufficient safeguards capable of ensuring effective protection of data subjects against risks of misuse (see no. 50-51, 56, 66).

115. The categories of data targeted by the draft 5th AML Directive. As indicated, the draft 5th AML Directive prescribes to collect and retain two main categories of data, being the customer identification data (see no. 87-95) and the beneficial ownership data (see no. 98-99). The first category primarily targets to obtain information capable of fully and precisely identifying the individuals involved in certain financial relationships and transactions, as well as to unravel certain specific features thereof. The second category aims to further identify the ultimate owners of companies, trusts and similar legal structures that are active in the Union’s financial sector.

As the gathering and monitoring of these data could indeed reveal suspicious payments and their (ultimate) beneficiaries, the required link with the purposes of preventing and detecting terrorist financing and money laundering offences can indeed be argued. However, the consequences of the retention of these particular data in terms of privacy invasion may not be underestimated. Essentially, the draft 5th AML Directive asks the obliged entities to set up (major) data bases encompassing the payment records of their clients (which they, certainly in the context of enhanced customer due diligence measures, must supplement with various additional information), and obliges the Member States to put in place an even wider data base gathering beneficiary information pertaining to almost all entities (see no. 87 and 99). As the obliged entities, moreover, have been left room to adopt broad interpretations of the data they may collect, it is certainly not inconceivable that, in the end, detailed and intrusive outlines of a person’s liquidity management, both conducted online and offline, are being collected and retained on the basis of the draft 5th AML Directive.

In this respect, it can be argued that the latter instrument should have offered the Member States, and moreover the obliged entities, some more clear and precise guidance as to how far they can go and which limitations they have to respect with regard to the categories of data that can be collected. Along the same lines, the European legislator can be reproached to have refrained from implementing adequate safeguards preventing excessive collection of a wide array of data.

Secondly, it must be highlighted as well that within the context of the customer due diligence measures, the draft 5th AML Directive also provides for the collection and processing of ‘sensitive data’, since it requires the obliged entities to verify whether an individual is, or has become, a ‘politically exposed person’ (see no. 95). Hence, the political opinions of data subjects’ are being processed, which must in essence follow stricter rules in terms of data protection. Principally, the

274 Draft 5th AML Directive, Art. 11(e); 13(1)-(2); 18a and 32a(3a).
processing of such data is even prohibited unless one of the circumstances of Article 9(2) GDPR can be demonstrated. In the presented case, the data processing could be argued to be lawful in the light of Article 9(2)(g) GDPR, on the condition that the monitoring of one’s political involvement is necessary for reasons of substantial public interest and when specific measures to safeguard the fundamental rights and interests of the data subjects are provided. However, one can rightfully question whether the draft 5th AML Directive fulfils these conditions, since certainly the establishment of specific safeguards, protecting against the misuse of these sensitive data, seems missing. Along the same lines, the CJEU’s stressed in its Opinion 1/15 that processing of sensitive data must be based on precise and particularly solid grounds other than the protection of public security against terrorism and serious transnational crime (see no. 64). Again, the demonstration of such further going reasons is, however, nowhere in the draft Directive to be found.

116. **The means of payment targeted by the draft 5th AML Directive.** Secondly, it is likely that the Court would examine as well whether the “means of payment”\(^ {275}\) that are targeted by the draft 5th AML Directive are also limited to what is strictly necessary to achieve the pursued objectives. In this regard, a reference should be made to paragraphs 79-81 and 85-86, which respectively discuss the range of obliged entities and the transactions subjected to the customer due diligence measures, as this also gives a notice of the means of payments that are being monitored. Especially in the light of the new channels that are addressed by the draft 5th AML Directive (see no. 79), it seems safe to say that the affected means are again extensive. However, the focus of this thesis lies, *inter alia* for reasons of space, elsewhere.

117. **The data retention period envisioned by the draft 5th AML Directive.** Thirdly, in view of both the CJEU’s settled case law and the storage limitation principle contained within the GDPR\(^ {276}\), also the period for which the personal data may be retained must be clearly specified and limited to what is strictly necessary to pursue the said objectives.

For both the customer identification and the beneficial ownership data, the draft 5th AML Directive principally adheres a data retention period between five and ten years after respectively the end of the concerned business relationship or transaction (see no. 96) and the removal of the beneficial ownership information from their relevant registries (see no. 100). From the CJEU’s case law, it can be deducted that the compatibility of a certain data retention period with the Union’s data protection regulations depends on the specific circumstances of the case. It is to say, where the CJEU in the judgement of *Digital Rights Ireland* objected to a data retention period between six and

\(^{275}\) By analogy with the “means of communication”, see no. 56.

\(^{276}\) GDPR, Art. 5(1)(e).
twenty-four months (see no. 50), it expressed not to experience difficulties with the data retention period of five years concluded in the PNR Canada Agreement (see no. 67). However, as in the presented case the foreseen retention period only starts running after the, initially accepted, transaction or business relationship has ended, a retention period of five (and certainly of ten) years, irrespective of whether or not the concerned relationships or transactions were by any means perceived suspicious, seems rather problematic in the light of the Union’s data protection framework. Indeed, in Opinion 1/15 the CJEU ruled that the retention of PNR data, after the data subject had left the country and was found not suspicious, could only be based on objective criteria demonstrating a clear connection between the retained data and the pursued purposes. As the customer identification and beneficial ownership data appear however to be retained in bulk, such link does not seem to exist in the presented case.\(^{277}\) Hence, the envisioned data retention period should only be maintained with respect to data of those who could in some way be associated with, or could contribute to the fight against, crimes of terrorist financing or money laundering.

118. The data subjects targeted by the draft 5\(^{th}\) AML Directive. Last and most importantly, also the public whose personal data are collected and retained must be limited to what is strictly necessary in order to counter terrorist financing and money laundering offences. In this respect it has been reiterated over and over again that only individuals whose data are likely to reveal a link with the targeted crimes can be subject to the data processing concerned (see no. 50, 56 and 66). Accordingly, on this point the draft 5\(^{th}\) AML Directive seems to encounter a considerable degree of hardship.

With regard to the customer identification data, it must be specifically clear that each and every client of the wide range of obliged entities is targeted by the data retention obligations, in first instance when they engage in a business relationship with the obliged entity, and then again when they carry out one of the targeted transactions (see no. 85-86). Considering the fact that both the obliged entities and the specific transactions triggering the collection of customer due diligence information are defined in a (very) broad way, the data processing practices imposed by the draft 5\(^{th}\) AML Directive start to bear, with respect to ‘the public affected’, a strong resemblance to the general and indiscriminate data processing provisions that are explicitly prohibited by the CJEU in its judgements of Data Rights Ireland and Tele2 Sverige AB (see no. 50 and 56). Moreover, it must be highlighted that those clients are (less or more closely) monitored throughout their entire

\(^{277}\) In this regard, it must, moreover, be noted that practise shows that the obligation to delete the personal data after the said retention periods have expired, is often overlooked by many AML/CTF professionals: Sana Khan, ‘The Fourth AML Directive and the EU’s Approach to Data Protection: A Precautionary Warning’ (\textit{ACamsToday}, 15 July 2016) [https://www.acamstoday.org/fourth-aml-directive-eus-approach-to-data-protection/] accessed 8 April 2018 [‘Sana Khan, ‘The Fourth AML Directive and the EU’s Approach to Data Protection’].
relationships as well, again without the prior demonstration of any link with, or contribution to, terrorist financing or money laundering being necessary. Hence, the existence of clear and precise rules, based on objective and well-evidenced criteria, delineating the public affected seems difficult to argue. Admittedly, the preamble of the Directive is endowed with justifications as to why certain obliged entities and certain transactions are included in its scope, but together all these entities and transaction seem to cover almost every individual.

Secondly, also with regard to the beneficial ownership data, the comprehensive character of the targeted data subjects cannot be denied, as every beneficial owner of every corporation, trust and similar structure is, without any differentiation, targeted by the concerned provisions as well (see no. 98).

However, by means of providing some counterweight to these made observations, the opening left by the CJEU in its Opinion 1/15 for the collection (and transfer) of personal data in bulk, without any link as such with terrorism, must be pointed out as well (see no. 64). Although the mechanism used in the PNR Canada Agreement was not quite the same as that envisioned by the draft 5th AML Directive, it can nevertheless not be ruled out that the CJEU again accepts the general collection and monitoring of (this time customer identification and beneficial ownership) data, with a view to filter out suspicious transactions and individuals at a later stage. However, it needs to be noticed that the Court’s Opinion 1/15 must, as indicated, be seen as a product deriving from the particular circumstances of the case, giving by no means a guaranteed permission to carry out general data processing practices (see no. 64).

That being said, some further insights with regard to two crucial specificities of the draft 5th AML Directive will be delivered, as they need additional attention in the light of the data protection laws.

Firstly, it is important to highlight that, where the filtering of 'suspicious' transactions and individuals is being proceeded by automated means, again stronger safeguards should be implemented and stricter data protection rules must be abided by the obliged entities, inter alia, to mitigate the persistent margin of error. Such includes, amongst others, the establishment of non-discriminatory, specific and reliable pre-established models and criteria and the arrangement of human intervention before taking individual measures based upon the automated processing (see no. 65). Given the serious consequences of the label ‘suspicious’ (even the termination of the concerned business relationship or transaction, see no. 91), the provision of such safeguards is particularly important in

278 Digital Rights Ireland, para 55.
the presented case. Again, the draft 5th AML Directive provided, however, no real examples of how these stronger safeguards should look like, fully leaving it up to the discretion and willingness of the Member States and/or obliged entities themselves to seek the necessary balance between the AML requirements and the requirements imposed by the Union’s data protection framework.

Secondly, also the requirement of the draft 5th AML Directive to put an increased focus on certain transactions and individuals necessitates a particular emphasis and scrutiny in terms of data protection. Indeed, it is clear that those subjected to enhanced customer due diligence measures have to endure (even more) intrusive collection and processing of their personal data and are in that respect ‘extra targeted’ by the draft 5th AML Directive (see no. 93-95). In that context, it is self-evident that the limitation of the data subjects to those whose data are likely to reveal a link with money laundering or terrorist financing, or could contribute to the prevention hereof, becomes even more important and that no exceptions should be made anymore. Hence, it must be examined whether the draft 5th AML Directive provides for both sufficiently clear and precise rules that, based on objective criteria, delineate the concerned categories of data subjects, as well as for sufficient safeguards protecting them against misuses.

In this regard, primarily the enhanced monitoring of politically exposed persons and their families seems delicate. Surely, it may well be wondered whether one’s choice (or one’s father’s choice) to participate in the political debate can be considered to constitute an objective criteria pursuant to which a detailed investigation and storage of his or her payments can be justified. This is even more true since the legislator drafted a rather broad interpretation of ‘politically exposed persons’ (Annex, (iv)). Hence, not only individuals truly engaged in politics are subject to the increased monitoring, but also inter alia certain judges and board members of international organisations will have to endure the more elaborated monitoring and storing of their financial operations. Accordingly, a more narrow interpretation of ‘political exposed persons’, or (once again) the inclusion of concrete and adequate safeguards would probably be more in line with the principle of proportionality enhanced in Article 52(1) of the EU Charter and Article 5(1)(c) GDPR.

Lastly, the draft 5th AML Directive also enables obliged entities themselves to determine other cases of ‘higher risk’ that demand for enhanced customer due diligence measures (see no. 93), and puts in that respect again high responsibilities with the quoted entities to establish anti-money laundering and terrorist financing provisions while respecting the Union’s data protection rules. In this regard, it must be noted that the ‘risk-based approach’, which the obliged entities must adopt to determine
these high-risk cases\textsuperscript{280}, encompasses a system of profiling of the concerned clients (see no. 95).\textsuperscript{281} Consequently, again stricter rules and stronger safeguards in terms of privacy and data protection should be put into place. However, an explicit reminder hereto and some additional guidance by the draft 5\textsuperscript{th} AML Directive in this respect are, although appropriate, again left out. Also the EDPS already criticized the vagueness with which the draft Directive describes the criteria selecting the categories of customers who necessitate enhanced control.\textsuperscript{282}

119. Accordingly, the proportionality and necessity of the collection and retention of the customer identification and beneficial ownership data prescribed by the draft 5\textsuperscript{th} AML Directive appears in general debatable. The combination of the comprehensiveness of the ‘public affected’, the number of intrusive data processing aspects (processing of sensitive data, using automated systems, profiling of data subjects\textsuperscript{283}, retaining the data for a long period after the transactions were declared unsuspicious) and the lack of concrete and adequate safeguards mitigating such intrusive processing, leads to the impression that the data collection and retention operations imposed by the draft 5\textsuperscript{th} AML Directive are not limited to what is strictly necessary to combat terrorist financing or money laundering.

\textit{b.ii. Access to and use of the collected personal data}

120. At least equally important is that also the subsequent phases of access to, and use of, the collected customer identification and beneficial ownership data must stay limited to what is strictly necessary to achieve the pursued objectives of countering terrorist financing and money laundering. Also in this respect, the CJEU has ruled in clear wording that general access to all retained data can never be regarded as limited to what is strictly necessary and emphasized that access to the collected personal data may only be granted with regard to individuals who are suspected of being in some way involved in the targeted serious crimes, or with regard to those whose data is likely to contribute to combating such activities (see no. 50, 57 and 66). Moreover, the CJEU has argued that, also in the other direction, a link should exist between the entities who may access the data and the pursued objectives, to the extent that the latter’s functions must somehow be related to the said purposes (see no. 66).

\textsuperscript{280} And to determine which existing clients should be subject to further customer due diligence measures: draft 5\textsuperscript{th} AML Directive, Art. 14(5).
\textsuperscript{281} Advies privacy Commissie, 37.
\textsuperscript{282} EDSP Opinion 5\textsuperscript{th} AML Directive, 50.
Again the legislator must provide for clear and precise rules that, based on objective criteria, indicate the circumstances in which personal data are accessible to ensure the above, as well as for specific safeguards protecting the interests of the data subjects concerned.

121. However, having examined the draft 5th AML Directive’s provisions governing the access to the personal data gathered within its context, it cannot be denied that the envisioned access possibilities deviate to a great extent from those advocated by the CJEU. Difficulties can be identified in relation with two main aspects.

122. Firstly, it must be reminded that both the customer identification and the beneficial ownership data are practically fully accessible to both FIU’s and competent authorities (see no. 97 and 101). Especially with regard to the customer identification data, the mechanism that in this context is established (the obliged entities principally notify suspicious transactions and the thereto-related customer identification data to the competent FIU, see no. 97) seems, at least at first sight, to indeed exhibit the required link between the accessed data and the pursued objectives. However, data protection issues have, nevertheless, slipped into the draft 5th AML Directive trough the unrestricted character of the access FIU’s (and essentially also the competent authorities) are offered to use the gathered data (see no. 97). Indeed, in contrary to what the 4th AML Directive provides for, FIU’s will be granted the right to obtain (additional) information on financial transactions, not only when justified by previous suspicious transactions reported to the FIU, but also through other means such as, inter alia, the FIU’s own analysis and intelligence.

By doing so, the draft 5th AML Directive clearly eliminated important safeguards that secured the required double link discussed above and provided some extent of proportionality. Also the EDPS warned in this respect for the undesirable shift from a targeted investigation-approach to an approach closely resembling to data mining, which is of course much more cautious treated in the light of the Union’s data protection law and requires again additional safeguards that, however, do not seem to be integrated in the draft 5th AML Directive.

123. A second set of serious concerns relates to the broad access possibilities that are offered to the obtained beneficial ownership data, since, next to the FIU’s, competent authorities and obliged entities, also ‘every member of the general public’ may access these data (see no. 101). Indeed, the draft 5th AML Directive envisions to further expand the public accessibility of beneficial ownership

284 Draft 5th AML Directive, Art. 32(9) and rec. 14. This recital only requires information requests to be based on ‘sufficiently defined conditions’. See also: Commission Action Plan, 7.
data in two important aspects, making it hardly arguable that the granted access is still limited to what is strictly necessary to fight terrorist financing or money laundering.

124. First of all, the draft 5th AML Directive resolutely abolishes the safeguard of having to demonstrate a ‘legitimate interest’ for members of the general public to obtain access to the beneficial ownership data of corporations and other legal structures. In other words, everyone will be able to access and use the beneficial ownership information of every company, for whatever reasons they might contrive and without any control possible as to what they essentially do with the found information. Hence, together with the removal of the ‘legitimate interest-safeguard’, also the required link between the accessibility of the concerned data and the objectives of fighting money laundering or terrorist financing has disappeared. By making the beneficial ownership information accessible to the public at large without any conditions, the European legislator clearly refrained from limiting the concerned access to a necessary group of entities that are precisely designated and that dispose of the powers to effectively contribute to the fight against terrorist financing or money laundering. In this view, the EDPS rightfully pointed to the fact that the investigation and enforcement of criminal activities are reserved solely to the competent authorities. Private subjects or entities are, on the contrary, under no circumstance entrusted with any enforcement role and are merely requested to provide information to the competent authorities in charge. Hence, the EDPS questioned the necessity of providing access to beneficial ownership information to other entities than those entrusted with law enforcement competences pertaining to money laundering and terrorist financing offences, and consequently expressed in general its concerns as to proportionality of the draft 5th AML Directive and the public access envisioned therein.

Furthermore, it must also be clear that, with the establishment of public registers, the legislator not only failed (again) to implement (or even to simply preserve) essential safeguards capable of protecting the interests of the data subjects against risks of misuse, it even made it impossible for the obliged entities to do so themselves. Indeed, as the EDPS rightfully pointed out, the requirement to introduce safeguards and controls against, *inter alia*, misuse or theft of personal data, does not

---

286 EDSP Opinion 5th AML Directive, 16.
287 EDSP Opinion 5th AML Directive, 64 In this regard, the EDPS acknowledged that NGO’s working on financial crimes and abuses, the press and investigative journalism indeed in certain circumstances can draw the attention of the authorities to criminal practises, but advocated thereupon that these interests *de facto* constitute a component of the right to obtain and to provide information, and thus serves distinct purposes. Accordingly, the proportionality of such rule should be assessed against that right and not against purposes of fighting money laundering and terrorism: EDSP Opinion 5th AML Directive, 62.
288 EDSP Opinion 5th AML Directive, 64
289 Repeatedly requested by both the CJEU and the sixth data protection principle of data integrity and confidentiality: GDPR, Art. 5(1)(f).
apply to personal information processed or controlled by individuals. Consequently, one may well wonder how the public at large could ever be stopped from misusing the personal information about a beneficial owner they have obtained from one of the registers.

Finally, the discontent of the CJEU with regard to the public registers can particularly be anticipated by referring to its Opinion 1/15, which also dealt with public access to personal data. In this opinion, the CJEU already found the access granted to members of the general public with the requirement of having a legitimate interest to exceed the limits of what was strictly necessary because of a lack of specifications and delimitations as to, *inter alia*, the persons to whom a disclosure of the personal data could be made; the use that is to be made of the concerned information; the terms ‘legitimate interests of the individual concerned’; and the purpose of the disclosure to the individual, which must moreover, according to the Court, demonstrate a link with the pursued objectives (see no. 68). Furthermore, the CJEU mandated that a disclosure of personal data to individuals must be conditional on the authorization of a judicial authority or an independent administrative body (see no. 68). Realizing that the public access predetermined by the draft 5th AML Directive includes, as indicated, none of these data protection requirements, and even removed the only safeguard of demonstrating ‘legitimate interest’291, the latter instrument is doing an even worse job in the terms of data protection than the PNR agreement did, which got invalidated.

125. With regard to the beneficial ownership data of trusts and similar structures, the draft 5th AML Directive newly established ‘public access’ as well, admittedly whilst preserving the safeguard of demonstrating ‘legitimate interest’ this time (see no. 101). However, before applauding too soon, two remarks must be made which cause the concerns expressed above to, at least to a considerable extent, apply with respect to trusts as well.

Firstly, it must be pointed out that the concept of ‘legitimate interest’ is defined rather broadly, again causing the required link between the accessible data and the objectives of the draft Directive to blur (see no. 98). Also the EDPS reproached the European legislator to, by defining the concept of legitimate interest in such a broad fashion, elicit ‘opportunistic behaviour’ of individuals who want to access the valuable beneficiary information for merely opportunistic reasons.292

A second remark criticizes the explicit possibility that the draft 5th AML Directive has left for the Member States to establish even wider access to the beneficial ownership information of (some

290 EDPS Opinion 4th AML Directive.
291 Also the EDPS referred to the requirement of holding legitimate interest as a safeguard for proportionality, since such a requirement “restricts the number of those entitled to access information”: EDSP Opinion 5th AML Directive, 57.
categories of) trusts and similar structures\textsuperscript{293}, as this provision seems to authorize Member States to simply do away with the ‘legitimate interest’-safeguard after all, and to put trusts in the same \textit{unfavourable} position as all other companies.\textsuperscript{294} Again this has not escaped the attention of the EDPS, who considered the quoted possibility to endanger the legitimate implementation of the draft 5\textsuperscript{th} AML Directive by the Member States in the light of the proportionality principle. It primarily labelled the left opportunity as a possible excuse for the Member States to enable “public scrutiny” against tax evaders\textsuperscript{295}, and again regretted the abstention of the European Council to provide any guidance as to the application of data protection safeguards.\textsuperscript{296} In this view, the EDPS further rightfully pointed out that mere references to the applicability of the data protection rules and the need for the Member States to respect these provisions, are not \textit{as such} sufficient to accept the compatibility of the draft 5\textsuperscript{th} AML Directive with the Union’s data protection framework.\textsuperscript{297}

126. Lastly, it needs to be reminded that, as regards the phase of access to collected personal data in general, the CJEU explicitly established and reiterated a number of specific safeguards with which regulators have to provide their legislations in order to protect the data subjects concerned against misuses of their accessed data (see no. 50, 57 and 66). A highly valuable aspect hereof demands that the access to obtained personal data is generally subjected to a prior review carried out by a court or an independent administrative body. However, neither with respect to the customer identification data, nor with regard to the beneficial ownership data, this demand was heard by the draft 5\textsuperscript{th} AML Directive. Indeed, by making the beneficial ownership registers and the therein-contained personal information freely available for all to see, the EU Council and Parliament could not have moved further away from the quoted data protection requirement.

127. Accordingly, it cannot be denied that the European legislator dropped more than a few stitches in terms of EU data protection demands when drafting the 5\textsuperscript{th} AML Directive and the access possibilities contained therein. The envisioned significant expansion of the accessibility of the customer identification and beneficial ownership data, without on the other hand providing for sufficient and adequate safeguards to counter the equally increased risks of misuse, is truly endangering the proportionality of the draft 5\textsuperscript{th} AML Directive.\textsuperscript{298} The EU Council and Parliament

\begin{flushleft}
\textsuperscript{293} Draft 5\textsuperscript{th} AML Directive, Art. 31(3)-(4).
\textsuperscript{294} The preamble of the draft 5\textsuperscript{th} AML Directive justifies the given national discretion as necessary in view of the varying characteristics that different forms of trusts can entail, which associate with different degrees of risks in terms of money laundering and terrorist financing: draft 5\textsuperscript{th} AML Directive, rec. 22.
\textsuperscript{295} EDSP Opinion 5\textsuperscript{th} AML Directive, 41.
\textsuperscript{296} EDSP Opinion 5\textsuperscript{th} AML Directive, 41. Also in the literature, the Union’s negligence to precisely clarify how organizations must combine their AML and data protection requirements was criticized: Sana Khan, ‘The Fourth AML Directive and the EU’s Approach to Data Protection’
\textsuperscript{297} Draft 5\textsuperscript{th} AML Directive, rec. 22a.
\textsuperscript{298} EDSP Opinion 5\textsuperscript{th} AML Directive, 3.
\end{flushleft}
blatantly failed from offering access to the collected personal data only when such is necessary in view of the fight against money laundering and terrorist financing. By doing so, they cause significant and unnecessary risks in view of the respect for the fundamental rights to privacy and data protection of the (numerous) data subjects concerned.

Hence, in order to ensure a sufficient degree of proportionality, the introduction of precise and well-funded prerequisites governing the access to financial transactions and beneficial ownership information by FIU’s, competent authorities and the public at large appears indispensable. Preserving—and narrowly defining—the requirement of ‘legitimate interest’ in case of this latter category seems in this respect the least we can do. Solely granting access to the beneficial ownership registers to entities that are in charge of enforcing the law would be even better.299 Moreover, an independent administrative body or court should be appointed to verify the fulfilment of all implied conditions and safeguards.

b.iii. Purpose limitation principle

128. Finally, given the importance of the principle of purpose limitation, as a decisive factor of the proportionality test300 and a crucial aspect of both the fundamental right to data protection301 and the data protection principles harboured by the GDPR302, a distinct examination of the fulfilment hereof seems appropriate. From the outline, it can be said that the combination of the ‘blanket measures’303 and the lack of adequate safeguards discussed above, which currently define the draft 5th AML Directive, impede the latter instrument from ensuring that the personal data obtained on its basis are not further processed in a manner that is incompatible with the purposes of preventing money laundering or terrorist financing, unless such is necessary and proportionate to achieve certain other legitimate objectives (see no. 29-32).304

129. Admittedly, at first sight the draft 5th AML Directive actually seems to fully respect the purpose limitation principle, as it included almost a literal reflection of it amongst its provisions.305 However, in the cold light of the day the concerned provisions must be relativized by the

---

300 EU Charter, Art. 52(1).
301 EU Charter, Art. 8(2).
302 GDPR, Art. 5(1)(b).
303 These exact words were used by the EDPS: EDSP Opinion 5th AML Directive, 49. In this regard, it must be noted that the Article 29 Working Party have stated that ‘blanket measures’ are contrary to the principle of proportionality: Article 29 Data Protection Working Party, ‘Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector’ [2014] WP 211 <http://www.dataprotection.ro/servlet/ViewDocument?id=1081> accessed 10 April 2018 [WP, ‘Opinion 1/2014’].
304 GDPR, Art. 23(1).
305 Draft 5th AML Directive, Art. 41(2) and rec. 43.
acknowledgement that the draft 5th AML Directive essentially lacks the tools to genuinely enforce the principle referred to. Indeed, together with the discussed expansion of the access to the gathered personal data, the much needed safeguards that existed to keep further processing within the lines of the Directive’s objectives were removed as well.

First and foremost, it particularly seems impossible to reconcile the purpose limitation principle with the unconditional public access that is granted to the beneficial ownership information of companies. Refraining from exercising any control as to the reasons one relies upon to access the collected data, the draft 5th AML Directive can by no means ensure that the collected data are not further processed for purposes incompatible with combatting money laundering or terrorist financing. Also with regard to trusts, full compliance with the purpose limitation principle cannot be ascertained given the above-mentioned broad definition that is being given to the concept of ‘legitimate interest’ and the envisioned possibility of the Member States to even completely abolish the quoted safeguard after all (see no. 125).

Secondly, also the unrestricted access of which the FIU’s and competent authorities dispose to, even on own initiative, process the customer identification and beneficial ownership data (see no. 97 and 101) seems irreconcilable with the purpose limitation principle, since the competences with which notably these last entities are entrusted exceed tasks of detecting, investigating and prosecuting solely crimes of terrorist financing and money laundering. Indeed tax authorities are offered the same level of unrestricted access to the obtained data as well (see Annex, (viii)). Hence, it can again not be guaranteed that these entities refrain from processing the accessed data for reasons other than, and incompatible with, the mentioned crimes. Moreover, the EDPS rightfully noticed in this regard that if the listed processors indeed act for different purposes, “such purposes do not appear sufficiently specified”.

Finally, when discussing the draft 5th AML Directive in the light of the purpose limitation principle, it is highly important to keep in mind that, although not explicitly expressed by the draft Directive, the increased access possibilities were indeed for a large part guided by reasons other than countering terrorist financing or money laundering offences. It is to say, the Commission figured to use the revision as a chance to pick up the fight against tax evasion as well (see no. 75). Hence, the processing of the gathered data for such purposes can certainly be anticipated. In this regard, it must be admitted however that further processing for tax reasons can enjoy a sort of exceptional treatment in the light of the purpose limitation principle, since it can be accepted on the

306 Also the EDPS pointed to these difficulties: EDSP Opinion 5th AML Directive, 36.
condition that such processing is, on itself, considered *necessary* and *proportional* to achieve the particular objectives of tax evasion (see no. 31).³⁰⁸

However, where this thesis, for the reasons expressed above, already doubts the proportionality of the indicated data processing practices in the light of the expressed objectives of fighting terrorist financing and money laundering, which belong to the most serious crimes, it certainly questions the proportionality of those practices for (merely) tax reasons. In this regard, also the EDPS voiced its concerns regarding such proportionality, asking why “*certain forms of invasive personal data processing, acceptable in relation to anti-money laundering and fight against terrorism, are necessary out of those contexts*”.³⁰⁹

131. Accordingly, also in this view, the EU Council and Parliament seem to have failed to do what was expected from them in order to comply with the data protection regulations, and refrained from protecting the Union’s citizens against the further processing of their customer identification and beneficial ownership data for purposes that are incompatible with the famous objectives of fighting the severe crimes of money laundering and terrorist financing.³¹⁰

Conclusion

132. An examination of the draft 5th AML Directive reveals a number of difficulties which threaten its compatibility with the fundamental rights to privacy and data protection, as well as with several key data protection principles harbouried by the GDPR (the principles of purpose limitation, data minimization, storage limitation and the principle of integrity and confidentiality). In general, the draft Directive appears characterized by a number of ‘blanket measures’ incapable of, on the one hand, assuring that the collection of, and access to, both customer identification and beneficial ownership data is limited to what is strictly necessary in view of fighting terrorist financing and money laundering offences, and of, on the other hand, ensuring that the concerned data are not wrongfully processed for reasons incompatible with the quoted ones. Moreover, the Council and Parliament clearly put only a minimum level of effort into establishing sufficient and adequate safeguards to protect the Union’s citizens against risks of misuse of their personal data enabled by

---


³⁰⁹ EDSP Opinion 5th AML Directive, 3. For example, the EDPS found the risk-based approach way less relevant in the context of the fight against tax evasion: EDSP Opinion 5th AML Directive, 51.

³¹⁰ See also: EDSP Opinion 5th AML Directive, 40; Advies Privacy Commissie, 17.
those blanket measures.\textsuperscript{311} Indeed, mere references to the applicability of (certain) data protection rules will not do the trick when the draft 5\textsuperscript{th} AML Directive does not allow their translation into facts.

\textbf{133.} Accordingly, if the draft 5\textsuperscript{th} AML Directive wants a chance of withstanding the CJEU’s assessment, if this latter was offered such an opportunity, some last-minute amendments mitigating the quoted irregularities seem crucial. More particularly, it is up to the European Council to further develop the indicated open and vague measures by using more precise and clear rules that reintroduce the repeatedly required link between the data processing practices and their pursued objectives and by subsequently endowing them with adequate safeguards, especially on the points were the data processing provided for by the draft 5\textsuperscript{th} AML Directive appears the most intrusive and the most delicate. In this last regard, additional attention must particularly be devoted to the provisions pertaining to the processing of sensitive data (see no. 115); the processing on grounds of automated means (see no. 118); practices of profiling (see no. 118); and to the provisions establishing all-encompassing access possibilities (see no. 123-126). Hereby, the CJEU’s judgements discussed above provide the necessary directions.

\textbf{134.} Given the Union’s function as prime guardian and enforcer of its own data protection framework, it is crucial that the EU Council assumes this office and sets out much more elaborated instructions for the Member States on how to balance the AML requirements with the data protection obligations. However, if the Council were to decline this task, it will be up to the Member States to take charge and seek for the quoted balance themselves when implementing the provisions of the draft 5\textsuperscript{th} AML Directive into their national laws.

Lastly, it is clear that also the obliged entities will play a vital role in protecting and safeguarding their clients’ rights to privacy and personal data protection, since they too are offered a considerable amount of responsibilities and discretion when it comes to executing the requirements of the draft 5\textsuperscript{th} AML Directive.\textsuperscript{312} Hence, it will be crucial for the obliged entities to understand their responsibilities under both the draft 5\textsuperscript{th} AML Directive and the discussed data protection laws, and to ensure that they are striking the right balance between these two.

\textsuperscript{311} In this regard, also the key principle of integrity and confidentiality is not respected: GDPR, Art. 5(1)(f) GDPR. See also: WP, ‘Opinion 1/2014’, 10.

\textsuperscript{312} In the light of the GDPR, such becomes even more important as it introduces the concept of ‘individual accountability’: GDPR, Art. 5(2). See no. 40.
FINAL CONCLUSION

135. The draft 5th AML Directive builds upon the 4th AML Directive by strengthening the therein-contained transparency rules, eventually presenting a framework which, on the one hand, scrutinizes and keeps track of the financial transactions conducted by almost everyone active within the Union’s financial system, and, on the other, provides complete insight in the real ownership of companies, trusts, and similar legal structures. The draft Directive constitutes a clear expression of the increasing concern towards terrorism and of the subsequent tendency to closely monitor every being in that view, ensuring they are not engaging in any atrocities related thereto. However, it must be clear that, while closing the routes used for terrorist financing, the draft 5th AML Directive on the other hand undeniably further expands the channels through which huge volumes of personal data can (wrongfully) be collected and further processed.

As, nonetheless, besides the 4th AML Directive also the Union’s data protection legislation will soon be introduced in a substantially strengthened fashion, it is today more difficult, but also more important, than ever to find the right balance between both reinforced frameworks and their conflicting objectives. Regrettably, the draft 5th AML Directive does not seem to have succeeded in striking this fair balance. The performed assessment made it particularly clear that, in the attempt to act against the surge of terrorist attacks, the competent EU institutions repeatedly lost sight of the vital data protection laws and neglected the need to also protect their citizens against the significant dangers caused by intrusive data processing practices. Accordingly, the posed research question, examining whether the draft 5th AML Directive is compatible with the Union’s data protection framework, must be answered in the negative.

Hence, it is crucial that the EU Council finds the courage to make a range of eleventh-hour amendments to the draft 5th AML Directive, in order to take up its role as guardian of the Union’s data protection framework and to provide a well-deliberated version of the envisioned AML reinforcements, demonstrating the necessary respect for the fundamental rights to privacy and data protection, the key data protection principles contained within the GDPR and the Court’s settled case law.
BIBLIOGRAPHY

Primary sources

European Union legal sources

Primary legislation

Secondary legislation
European Union case law: Court of Justice of the European Union


- Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others [2016] ECLI:EU:C:2016:970;


- C-1/15 Opinion 1/15 EU-Canada PNR Agreement [2017] ECLI:EU:C:2017:592;


Council of Europe legal sources

- Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 5;


Belgian legal sources


Secondary Sources

European Council documents


European Parliament documents


European Commission documents

- Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’ COM(2012) 11 final;


- Commission, ‘Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security’ COM(90) 314 final;


**European Data Protection Supervisor (EDPS) documents**


Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 Working Party) documents


European Union Agency for Fundamental Rights (FRA)


Doctrine, websites and blogs


- Granger M-P and Irion K, The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU legislator and Teaching a Lesson in Privacy and Data Protection (Sweet & Maxwell 2014);


- Kuskonmaz E.M, ‘Following the digital footprints of airline passengers: An assessment of the EU-US PNR Agreement with respect to the EU right to privacy and data protection’ in Gert Vermeulen and Eva Lievens (eds), Data Protection and Privacy under Pressure (Maklu 2017);


- Murphy C, The EU Counter-Terrorism Law: Pre-Emption and the rule of Law (Hart Publishing 2015);

- Preziosi C, ‘Finding the balance between data protection and AML requirements’ (Lexology, 23 June 2017) <https://www.lexology.com/library/detail.aspx?g=8aabbfb8-33c1-456d-869b-ef1f56ec0e08> accessed 7 April 2018;

- Tracol X, ‘Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of


– Vermeulen G, ‘The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services’ in Svantesson, Dan J.B. and Dariusz Kloza (eds), Transatlantic Data Privacy Relationships as a Challenge for Democracy; European Integration and Democracy Series, vol 4 (Intersentia 2017).

Other


ANNEX: LIST OF DEFINED TERMS

Several concepts need to be clarified given their importance throughout this dissertation. Hereto, primarily the definitions as they appear in the concerned legislative instruments will be used.

Concepts related to personal data processing:

(i) **Personal data**: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.\(^{313}\)

(ii) **Sensitive personal data**: processing of ‘sensitive data’ implies the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.\(^{314}\)

(iii) **Data processing**: ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.\(^{315}\)

(iv) **Data controller**: ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.\(^{316}\)

(v) **Data processor**: ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.\(^{317}\)

\(^{313}\) GDPR, Art. 4(1).
\(^{314}\) GDPR, Art. 9(1).
\(^{315}\) GDPR, Art. 4(2).
\(^{316}\) GDPR, Art. 4(7).
\(^{317}\) GDPR, Art. 4(8).
(vi) **Processing by automated means:** ‘processing by automated means’, or using a ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.\(^{318}\)

(vii) **Profiling:** ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.\(^{319}\)

**Concepts related to the AML requirements:**

(i) **Money laundering offences:** ‘Money laundering’ is the processing of criminal proceeds to disguise their illegal origin. The crime of money laundering should apply to all serious offences, with a view to including the widest range of predicate offences.\(^{320}\)

(ii) **Terrorist financing offences:** ‘Terrorist financing offences’ extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.\(^{321}\)

(iii) **Beneficial ownership:** ‘beneficial owner’ means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. In the case of corporate entities it includes at least the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means (...). If, after having exhausted all possible means and provided there are no grounds for suspicion, no such person is identified, or

\(^{318}\) GDPR, Art. 4(6).
\(^{319}\) GDPR, Art. 4(4).
\(^{321}\) FATF Recommendations, 35.
if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s).\(^{322}\)

In the case of trusts it includes at least the settlor; trustee(s); the protector; the beneficiaries and any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.\(^{323}\)

In the case of legal entities such as foundations, and legal arrangements similar to trusts it includes at least the natural person(s) holding equivalent or similar positions as to those referred to in the previous paragraph.\(^{324}\)

(iv) **Politically exposed persons:** ‘politically exposed person’ means a natural person who is or who has been entrusted with prominent public functions and includes (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises and (h) directors, deputy directors and members of the board or equivalent function of an international organisation. On the other hand, it does not cover middle-ranking or more junior officials.\(^{325}\)

(v) **Family members of politically exposed persons:** ‘family members’ includes (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person and (c) the parents of a politically exposed person.\(^{326}\)

(vi) **Close associates of politically exposed persons:** ‘persons known to be close associates’ means (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person and (b)

\(^{322}\) Draft 5\(^{th}\) AML Directive, Art. 3(6)(a).

\(^{323}\) Draft 5\(^{th}\) AML Directive, Art. 3(6)(b).

\(^{324}\) Draft 5\(^{th}\) AML Directive, Art. 3(6)(c).

\(^{325}\) Draft 5\(^{th}\) AML Directive, Art. 3(9).

\(^{326}\) Draft 5\(^{th}\) AML Directive, Art. 3(10).
natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.\(^{327}\)

**(vii) Financial Intelligence Unit:** ‘FIU’s’ are operationally independent and autonomous central national units that are responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing.\(^{328}\)

**(viii) Competent authorities:** ‘Competent authorities’ are those public authorities with designated responsibilities for combating money laundering or terrorist financing, as well as tax authorities, supervisors of obliged entities and authorities that have the function of investigating or prosecuting money laundering, associated predicate offences and terrorist financing, tracing and seizing or freezing and confiscating criminal assets.\(^{329}\)

\(^{327}\) Draft 5\(^{th}\) AML Directive, Art. 3(11).

\(^{328}\) Draft 5\(^{th}\) AML Directive, Art. 32(3).

\(^{329}\) Draft 5\(^{th}\) AML Directive, Art. Articles 30(6)(2) and 31(4) *in fine.*