Strasbourg, 30 July 2021 T-PD(2021)4rev

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Report on the implications for data protection of mechanisms for inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes

by

Eleni Kosta

The opinions expressed in this document are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe

Contents

Abbreviations and acronyms

4AMLD	4th Anti-Money Laundering Directive (Directive 2015/849)
5AMLD	5th Anti-Money Laundering Directive (Directive 2018/843)
ACIP	Singapore AML/CFT Industry Partnership
AEOI	Automatic Exchange of Information
AML	Anti-Money Laundering
AUSTRAC	Australian Transaction Reports and Analysis Centre
BO	Beneficial Owner
CAA	Competent Authority Agreement
CDD	Customer Due Diligence
CDOT	United Kingdom Crown Dependencies and Overseas Territories International Tax Compliance Regulations
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108+	Council of Europe Modernised Convention for the protection of individuals with regard to the processing of personal data ETS No.108
CRS	Common Reporting Standard
CRS MCAA	Common Reporting Standard Multilateral Competent Authority Agreement
CTF	Countering the Financing of Terrorism
DAC	Directives on Administrative Cooperation
EBA	European Banking Authority
ECHR	European Convention on Human Rights
ECmHR	European Commission for Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EIOPA	Joint committee of the European Supervisory Authorities
EOIR	Exchange of Information on Request
ESMA	European Securities and Markets Authority
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FFI	Foreign Financial Institution
FIU	Financial Intelligence Unit
FMLIT	Hong Kong Fraud and Money Laundering Intelligence Taskforce
GDPR	General Data Protection Regulation
HIRE	Hiring Incentives to Restore Employment Act

IGA	Implementing Intergovernmental Agreements
IRS	US Internal Revenue Service
JMLIT	United Kingdom Joint Money Laundering Intelligence Taskforce
KYC	Know Your Customer
LED	The Law Enforcement Directive
LQDN	Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others v Premier Ministre and others* [2020] ECLI:EU:C:2020:791
MAC	OECD and Council of Europe Multilateral Convention on Mutual Administrative Assistance in Tax Matters
OECD	Organization for Economic Co-operation and Development
PPP	Public-Private Partnership
RIPA	United Kingdom Regulation of Investigatory Powers Act 2000
STR/SAR	Suspicious Transaction Report/ Suspicious Activity Report
TEU	Treaty on European Union
UBO	Ultimate Beneficial Owner
WP29	Article 29 Data Protection Working Party

1. Context

1.1 Introduction[1]

The exchange of information between various entities is cornerstone both as regards Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT), as well as for tax purposes. The facilitation of information sharing in the financial sector and for tax purposes has been high in the agenda of the Implementation Review Group of the Conference of the States Parties to the United Nations Convention against Corruption and attracted special attention as measure for exposing corruption during the Anti-Corruption Summit that took place in London in 2016.[2] In the financial sector the Implementation Review Group encouraged "all jurisdictions, where applicable national law permits, to improve information sharing between law enforcement authorities, FIUs, regulators and banks, and within and among private sector participants, both domestically and across borders"[3]. As part of their efforts to deter tax evasion and other tax crimes, they endorsed the implementation of "the Common Reporting Standard (CRS) on automatic exchange of information, which is vital for global tax transparency"[4].

The AML/CFT framework entails complex exchanges of data between customers, obliged entities, Financial Intelligence Units (FIUs) and law enforcement authorities, as well as intelligence services in some cases. As regards the field of taxation, the worldwide income taxation principle presupposes the exchange of information between various countries. Simply put "[r]esidence-countries taxing their residents on income produced both domestically and abroad need the cooperation of source-countries to obtain information about income produced by their residents in those countries".[5]

Traditionally, the focus in the exchanges of data both for AML/CFT and for tax purposes lies on the fight against economic crime. However, such exchanges usually encompass personal data, the protection of which needs to be respected. The need to align the AML/CFT requirements with the data protection ones has been recognised by the Financial Action Task Force (FATF) that recommended countries to enhance the cooperation and coordination between relevant authorities in order to ensure the compatibility of the AML/CFT requirements with data protection rules.[6] Similarly, the Global Forum on Transparency and Exchange of Information for Tax Purposes, an international body working on the implementation of global transparency and exchange of information standards around the world, places the importance of protecting personal data high in their agenda.

---

[1] I am very grateful to Sophie Kwasny and Bohumila Ottova of the Council of Europe for assisting with the preparation of this report. Lorena Ungureanu, Igor Nebyvaev, Benjamin Vogel, Magdalena Brewczyńska and Silvia de Conca provided very helpful comments on earlier drafts. I am also grateful to the members of the delegations who asked questions and provided comments on the earlier versions presented at the 40th Plenary (18_20 November 2020) and at the 52nd Bureau meeting (24-26 March 2021).

[2] UNODC, 'Anti-Corruption Summit: London 2016 Communiqué Document submitted by the Government of the United Kingdom' Seventh Session of the Implementation Review Group (20-24 June 2016) CAC/COSP/IRG/2016/CRP.19 <https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/20-24June2016/V1603744e.pdf> accessed 25 May 2021.

[3] Ibid, p.3.

[4] Ibid, p.5.

[5] Carlo Garbarino, 'The EU Protection of Tax Data Transferred to Third Countries' (2020) Bocconi Legal Studies Research Paper No. 3730009, p.1.

[6] FATF, 'Forty Recommendations' (October 2003), recommendation No. 2, < https://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf> accessed 25 May 2021.

1.2 The 2014 opinion on exchange of data

The Council of Europe has adopted Convention 141 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Convention 198 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.

At EU level, in 2011 the Council adopted the first Directive, Directive 2011/16, on administrative cooperation in the field of taxation (DAC). In 2012 the FATF revised its recommendations on AML/CFT, recommending, among others, monitoring and record-keeping of transaction data and sharing any relevant information with the requesting authorities domestically.

In response to this "new trend" to regulate exchanges of data, the Council of Europe adopted an opinion in 2014 on the implications for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes[7]. The 2014 opinion covered interstate exchanges only for administrative and tax purposes and only those that were automatic. According to the Organization for Economic Co-operation and Development (OECD), "the automatic exchange of information is understood to involve the systematic and periodic transmission of "bulk" taxpayer information by the source country to the residence country concerning various categories of income (e.g. dividends, interest, royalties, salaries, pensions, etc.)".[8] The automatic exchange of information is central in the field of exchange of tax information, as explained below, while the exchange of information for AML/CFT, especially as regards access of FIUs to data, can be done in various ways, as explained below.

The report that accompanied the 2014 opinion justified the linkage between the automatic exchange of personal data between States for administrative and tax purposes and similar exchanges aimed at combating money laundering on two main reasons:

> *Firstly, when revising its Recommendations in February 2012, the FATF decided to include "all serious offences" within the scope of AML/CFT, which encompass a large number of tax offences.*
>
> *The term "serious offences" used here reflects a drive to criminalise as many offences as possible by correlating the scope of anti-money laundering with the penalty applicable to the predicate offence. […]*
>
> *Secondly, it should be remembered that, in a 1998 report prepared in order to "develop measures to counter the distorting effects of harmful tax competition on investment and financing decisions and the consequences for national tax bases", the OECD determined four key factors in identifying tax havens: no or only nominal taxes, lack of effective exchange of information, lack of transparency and no substantial activities.*
>
> *Although tax havens have been heavily stigmatised in the political arena and in the media, it should be noted that the rudimentary aim of countering the distorting effects of international tax competition has now been transformed into a drive against fraud and tax evasion. Mistrust surrounding state practices in tax competition has now*

[7] Council of Europe, 'Opinion on the implications for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes' (4 June 2014) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806945a0> accessed 25 May 2021.

[8] OECD, 'Automatic Exchange of Information – What it is, how it works, benefits, what remains to be done' (2012) p. 7 <https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf> accessed 25 May 2021.

shifted to individuals. The exponential development of obligations and duties based on the notion of "suspicion" is remarkable in this connection.

So, as Europeans debate the issue of automatic inter-state exchanges of personal data for administrative and tax purposes, the imminent entry into force of Foreign Account Tax Compliant Act (FATCA) in respect of a great many countries has expedited the use of automated personal data processing permitting automatic exchanges of tax information.

As a result, the automatic exchange of information is becoming the international norm, as pointed out by the Secretary General of the OECD, who declared his satisfaction that "the political support for automatic exchange of information on investment income has never been greater. Luxembourg has changed its position and the US FATCA legislation is triggering rapid acceptance of automatic exchange and propelling European countries to adopt this approach amongst themselves. In response to the G20 mandate to make automatic exchange or information the new standard, the OECD is developing a standardised, secure and effective system of automatic exchange".[9]

1.3 Developments in the field of exchange of information

Since the adoption of the aforementioned 2014 opinion on the implications for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, the data protection framework both at the Council of Europe and at the European Union level was modified, with the adoption of the Modernised Convention 108 (or CoE Convention 108+) in 2018[10] and the adoption of the General Data Protection Regulation (GDPR)[11] and Directive 2016/680 (the Law Enforcement Directive or the LED)[12], which provides specific rules for the protection of personal data in the law enforcement context. The scope of the CoE Convention 108+ has been broadened and includes "both automated and non-automated processing of personal data (manual processing where the data form part of a structure which makes it possible to search by data subject according to pre-determined criteria) which falls under the jurisdiction of a party to the Convention".[13] In addition, the Court of Justice of the European Union has delivered a number of seminal judgments[14] that set a

---

[9] Caroline Porasso, Benjamin Aouizerat, 'Report on the implications for data protection of the growing use of mechanisms for automatic inter-state exchanges of personal data for administrative and tax purposes, as well as in connection with money laundering, financing of terrorism and corruption' (30 January 2014) < https://rm.coe.int/bureau-of-the-consultative-committee-of-the-convention-for-the-protect/168073dc57> accessed 25 May 2021.

[10] Council of Europe, Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data, (2018) CETS No. 223 < https://rm.coe.int/16808ac918> accessed 25 May 2021.

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

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

[13] Council of Europe, 'The Modernised Convention 108: Novelties in a nutshell' < https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8> accessed 25 May 2021.

[14] Joined Cases C-293/12 and C-594/*12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238; Joined Cases C-2013/15 and C698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Watson* [2016]

number of safeguards for the exchange of personal data that are relevant for the issue at hand and will be discussed later in this report.

At the same time, the exchanges of information in that context have heavily intensified and a complex framework of legal and regulatory instruments have been adopted, calling for a close focus on the fields of anti-money laundering and taxation.

1.4 Focus of this report

These developments call for a new opinion, an updated one that would address the data protection implications of data exchanges. While the 2014 opinion focused on data for administrative and tax purposes, the reference to administrative data remains very broad. This report focuses on exchanges of data for tax purposes and AML/CFT, instead. The exchange of data in the field of taxation is mainly realised between competent tax authorities and to a large extent it takes place in an automatic way, often without prior request. In the context of AML/CFT, however, the data are exchanged between various actors and in various ways. Keeping the focus on "automatic" inter-state exchanges would leave out crucial exchanges of data, especially in the field of AML/CFT. Consequently, the report will cover exchanges of data that are not necessarily automatic. It should be highlighted that there is a growing interest in the exchanges of data for AML/CFT and tax purposes within the same state, involving for instance Public-Private Partnerships in AML or data pooling for the private sector, which is one of the initiatives of the FATF under the German presidency.[15] Nevertheless, the nature of the issues are to a large extent different when the exchange takes place withing the same country, so this report deliberately covers inter-state exchanges. Thus, this report will focus on the implications for data protection of mechanisms for exchanges of data for AML/CFT and tax purposes.

This report will first present the exchange of data in the AML/CFT framework and in the field of taxation. It will then focus on areas that raise concerns regarding the legitimate processing of these personal data. It will thus examine the actors involved in these two fields from a data protection point of view. It will further elucidate on the data protection rights of the data subjects. The report will then analyse the legal basis that can legitimate the exchanges of data, before analysing the data protection principles (proportionality, fairness and transparency, purpose limitation, data minimisation, accuracy and storage limitation). The following section will briefly discuss data security issues while the last section will analyse the transborder data flows, which is of particular importance due to the focus of the report on "inter-state" exchanges. The report will conclude with some recommendations so that the interstate exchange of personal data for AML/CFT and tax purposes respects the principles and provisions of the CoE data protection framework.

ECLI:EU:C:2016:970; Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Data Protection Commissioner v Facebook Ireland, Maximillian Schrems* [2020] ECLI:EU:C:2020:559; C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [2020] ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others v Premier Ministre and others* [2020] ECLI:EU:C:2020:791 ; Joined Cases C-245/19 and C-246/19 *État luxembourgeois v B* and *État luxembourgeois v B,C,D,F.C* [2020] ECLI:EU:C:2020:795.

[15] FATF, 'Prioritised for the Financial Action Task Force (FATF) under the German presidency – Objectives for 2020-2022' (2020) <https://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf> accessed 25 May 2021.

2. Exchange of data in the AML/CFT legal framework

2.1 AML/CFT regulatory framework relating to exchanges of data

In 1990, the FATF introduced the first version of the "FATF Forty Recommendations"[16]. These were last thoroughly revised in 2012, integrating special recommendations on terrorist financing with the measures against money laundering, to build a comprehensive set of standards[17]. The FATF postulates that the state should criminalize money laundering and terrorist financing and involve the financial and other institutions in the prevention and reporting of money laundering. The tasks of prevention and reporting of money laundering by the obliged entities is realized primarily with the means of the customer due diligence (CDD).[18] The obligations imposed on the financial institutions are expressed via the "Know Your Customer" (KYC) requirement, i.e. identifying all customers, maintaining records of financial transactions; and informing Financial Intelligence Units (FIUs) of any suspicious activities through the reporting.

The FATF Recommendations contain a number of requirements on the exchange of information between financial institutions and the enabling of unhindered CDD and reporting. More concretely, Recommendation 9 requires countries to ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations. Recommendation 10 stipulates that "Financial institutions should be required to undertake customer due diligence (CDD) measures" in specific situations. The interpretative note to Recommendation 10 (Customer Due Diligence) clarifies with regard to enhanced CDD that: "Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.[19]

Recommendation 13 requires financial institutions, in relation to cross-border correspondent banking or similar relationships, to provide information about each other, beyond the performance of normal CDD measures. Recommendation 16 requires obliged entities to gather accurate information about their originator and beneficiary of wire transfers. Recommendation 17 sets out the requirements for the outsourcing of CDD to third parties (which may be based in another country) of customer identification data and of data relating to the purpose and intended nature of the business relationship. Finally, Recommendation 18 establishes a requirement for financial groups to share information within the group for AML/CFT purposes. The interpretative note to this Recommendation explains that such programmes should be applicable to all branches and majority-owned subsidiaries of the financial group and concern information required for the purposes of CDD and money laundering and terrorist financing risk management. Furthermore, it emphasizes the importance of adequate safeguards on the confidentiality and use of information, as well as points out that the scope and extent of this information sharing may be determined by the

---

[16] FATF, 'International Standards on Combating M3.oney Laundering and the Financing of Terrorism & Proliferation' (2020) < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 25 May 2021.

[17] Ibid.

[18] Ibid, Recommendation No. 10. See more on CDD in section 2.3.1.

[19] Ibid, interpretative note to Recommendation 10 (Customer Due Diligence), Para 20.

countries based on the sensitivity of the information, and its relevance to AML/CFT risk management.[20].

To increase international cooperation, the FATF recommends also monitoring and keeping records of cross-border financial flows and sharing relevant information with the requesting authorities. According to FATF "effective information sharing is one of the cornerstones of a well-functioning anti-money laundering/counter-terrorist financing (AML/CFT) framework".[21] Recommendation 35 suggests the establishment of a wide "range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative" that incentivise the performance of financial institutions and compliance in reporting suspicious activities. With that in mind the FATF, compiled the 25 FATF Recommendations that set out requirements on information sharing in a document titled a "Consolidated FATF Standards on Information Sharing"[22].

At the European Union level, the most important legal instruments relating to the exchange of data are Directive 2015/849 (4th Anti-Money Laundering Directive or 4AMLD)[23] and introducing modifications thereto, Directive 2018/843 (5th Anti-Money Laundering Directive or 5AMLD).[24] Directive 2019/1153[25] lays down measures to enhance access to and use of financial information and bank account information by competent law-enforcement authorities through providing them with a direct access to information contained in national centralised registries. It also facilitates access of the FIUs to the law enforcement information and stimulates access of investigative authorities to FIU data.[26] In May 2020 the European Commission published a Communication on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, where it expressed its intention to present new legislative proposals on AML/CFT.[27] The European Data Protection Board (EDPB) adopted a Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing[28] and addressed a letter to the

---

[20] Ibid, p.85.

[21] FATF, 'Consolidated FATF Standards On Information Sharing – Relevant excerpts from the FATF Recommendations and Interpretive Notes' (2017) <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/consolidated-fatf-standards-information-sharing.pdf> accessed 25 May 2021

[22] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2020) < https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-information-sharing.html> accessed 25 May 2021.

[23] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, p. 73–117.

[24] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, p. 43–74.

[25] Directive (EU) 2019/1153 of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.

[26] Ibid, Article 1(1).

[27] European Commission, Communication of 7 May 2020 on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, C(2020)2800 final (the "Action Plan") <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:C(2020)2800&from=EN> accessed 25 May 2021.

[28] European Data Protection Board, Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing (15.12.2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf> accessed 30 June 2021.

European Commission on the upcoming review of the European AML/CFT framework.[29] The EDPB highlighted that it is of utmost importance that "the anti-money laundering measures are compatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the principles of necessity of such measures in a democratic society and their proportionality, and the case law of the Court of Justice of the European Union"[30].

2.2 Exchange of information in AML/CFT

The exchange of information is important for the AML/CFT strategy. Data are collected by obliged entities and are transferred to FIUs, and subsequent investigative authorities, and to other obliged entities. The AML/CFT legal framework provides a number of concrete provisions on the exchange of information withing the AML/CFT context (see Figure 1). The data comes directly from a customer, who can be a physical or legal person, or from third parties, open source and potentially also commercially acquired non-open-source information. Should an obliged entity consider a transaction or an activity suspicious, it is obliged to submit a Suspicious Transaction Report (STR) (also known as Suspicious Activity Report (SAR)) to the FIU. This is usually the moment, when the data crosses the border between the private and public sphere. Such exchange can also take place when the FIU asks the obliged entity to provide information. Once the information from the STR is analysed by the FIU, the FIU usually looks at it in a broader context. To that end, the FIU can request follow up information addressed to reporting obliged entities, or to other obliged entities or even to foreign FIUs and other authorities.

Provided that the FIU concludes that the facts of the case would, in its eyes, justify the initiation of a criminal investigation, it shares the outcome of its analysis with the criminal justice authorities. Further exchange of information may take place at the level of sharing of financial intelligence with other authorities, such as tax or customs ones.

[29] European Data Protection Board, Letter to the European Commissioner for Financial services, financial stability and Capital Markets Union and to the European Commissioner for Justice (19.05.2021) < https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf> accessed 30 June 2021.

[30] European Data Protection Board, Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing (15.12.2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf> accessed 30 June 2021.

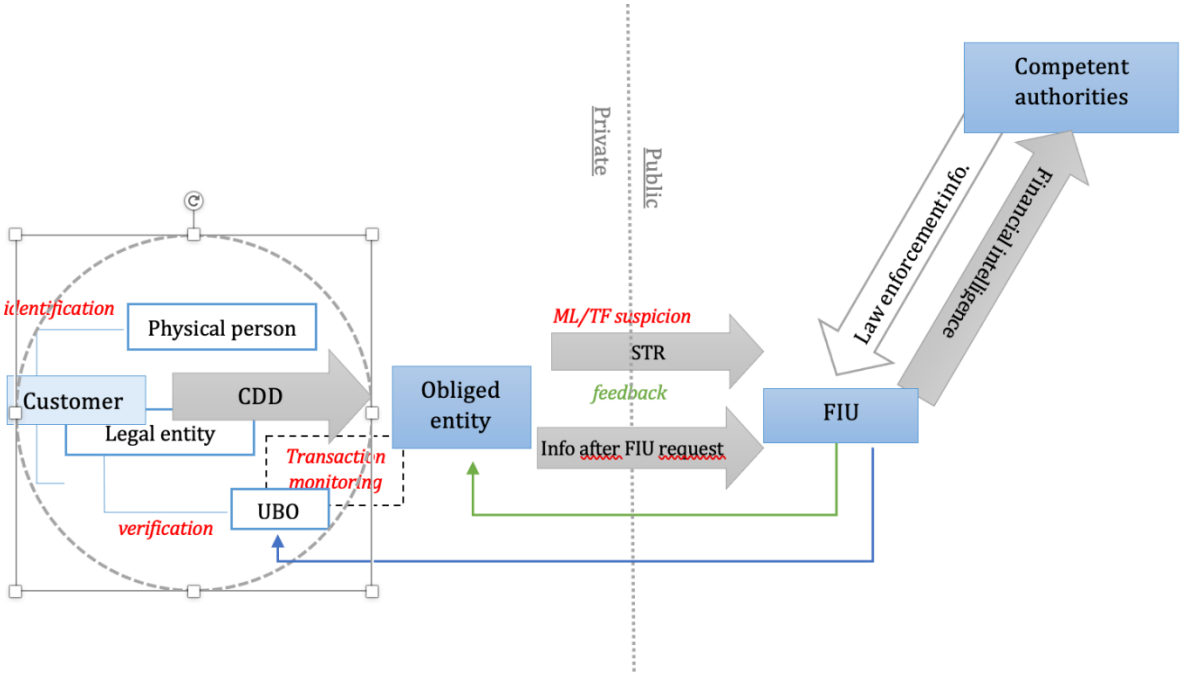

Figure 1 Basic flows of information in AML/CFT (Credit to Magdalena Brewczyńska)

Technological developments are enhancing the methods and techniques for the collection and analysis of data. Financial institutions are gradually adopting machine learning-based solutions, to complement and integrate rule-based tools. The combination of rule-based and risk-based approach uses many detection techniques to simplify and at the same time improve the detection process and implement CDD requirements to better understand who are the customers, their transactions and allow for more accurate identification of client risk.[31]

Machine Learning software are able to mine significant amounts of data to identify patterns, create profiles, cluster and categorize clients based on common features, and infer additional data in respect to those inputted. Machine Learning solutions can also be used by obliged entities to segment customers based on their risk category, and perform pattern analysis to detect anomalies in behaviour (either personalized on a specific customer or based on customer categories). They can also perform link analysis[32] to infer relationships among customers (network), or between customers and possible PEPs or watch-listed subjects, and to identify the Beneficial Owner (BO)[33] of a transaction or new account. At the same time there are questions raised whether AI-based AML systems are compatible with European fundamental rights.[34]

---

[31] Tamer Hossam and others, 'Design of a Monitor for Detecting Money Laundering and Terrorist Financing' (2016) 85 J
ournal of Theoretical and Applied Information Technology 425, 426. 9.

[32] Link analysis is a technique used to enquire into relationships among a large number of objects of various types. When used in money laundering, the objects may comprise of people, bank accounts, businesses, wire transfers and cash deposits. Scrutinizing associations between these various objects assists in indicating networks of activity, both legal and illegal. Cfr. US Congress, Office for Technology Assessment, *Information Technologies for the Control of Money Laundering* (US Government Printing Office 1995) 56 <https://docplayer.net/28783887-Information-technologies-for-the-control-of-money-laundering-september-ota-itc-630-gpo-stock.html> accessed 26 May 2021.

[33] According to Art.3(6) of the Directive 2015/849 (AMLD4): "'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". The article also provides with a list of specifications and explanations in case, for instance, of trusts or other business entities.

[34] Winston Maxwell, Astrid Bertrand, Xavier Vamparys. Are AI-based Anti-Money Laundering (AML)

Systems Compatible with European Fundamental Rights?. ICML 2020 Law and Machine Learning

2.3 Inter-state exchanges of data in the AML/CFT context

2.3.1 Customer Due Diligence

Customer due diligence (CDD) is a process in which the relevant information of an obliged entity's customer is collected and evaluated from the perspective of risk to money laundering or terrorist financing. Therefore, the realization of CDD is a primary source of information in the AML/CFT system. The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs)) published in 2017 guidelines on risk factors and simplified and enhanced customer dule diligence. These guidelines "provide credit and financial institutions with the tools they need to make informed, risk-based and proportionate decisions on the effective management of individual business relationships and occasional transactions for anti-money laundering and countering the financing of terrorism purposes. They provide guidance on the factors firms should consider when assessing the money laundering and terrorist financing risk associated with a business relationship or occasional transaction and set out how credit and financial institutions can adjust the extent of their customer due diligence measures in a way that is commensurate to the money laundering and terrorist financing risk they have identified"[35]. The CDD obligations require obliged entities to have in place adequate controls and procedures so that they know the customers with whom they are dealing and understand the nature of their business.[36] As part of the identification CDD measures, the obliged entities usually, as a minimum, identify their customers and verify their identity on the basis of documents, data or information obtained from a reliable and independent source. They also identify the beneficial owner and take reasonable measures to verify that person's identity so that the obliged entity knows who the beneficial owner is, in particular, as regards legal persons, trusts, companies, foundations and similar legal arrangements, and understanding the ownership and control structure of the customer. Furthermore, the obliged entities are required to obtain information on the purpose and intended nature of the business relationship.

Where a business or transaction involves a higher-risk of money laundering/terrorism financing (including when a third country involved in a transaction is considered high risk), obliged entities shall apply enhanced CDD measures, notably obtaining information on the customer or beneficial owner(s), intended nature of the business relationship, source of funds and source of wealth of the customer and of the beneficial owner(s). On the basis of CDD, customer risk-profiles are created and banks are required to periodically update customer data.

2.3.2 Information sharing within a group

Interstate exchange of information can already take place within a group of several undertakings, some of which can be established in another state. In such cases, these obliged entities are required to implement group-wide policies and procedures for sharing

---

Workshop, Jul 2020, Vienne, Austria. hal-02884824v3f.

[35] European Banking Authority, European Securities and Markets Authority and Joint committee of the European supervisory authorities, Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions - The Risk Factors Guidelines, 2018, available at https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence

[36] Eds. Colin King, Clive Walker, and Jimmy Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Laws* (Palgrave Macmillan, 2018) p.42.

information for AML/CFT purposes within the group they belong to.[37] Those rules shall be implemented effectively at the level of branches and majority-owned subsidiaries both in States Parties to the Convention and in third countries.

FATF recommendation 18 establishes a requirement for financial institutions to share information within the group for AML/CFT purposes. Such sharing of information shall be carried out in accordance with the safeguards established in Convention 108+ and the national legislation of the States Parties to the Convention.

A similar requirement can be found in Art. 45 4AMLD. At EU level, a group has been defined as "a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU".[38] Taking into account a possibility that a branch or a subsidiary of a credit or financial institution can be located in a third country, where the minimum AML/CFT requirements are less strict than those of the European Member State, and in order to avoid the application of very different standards within the institution or group of institutions, the obliged entities must apply the European Union standards or notify the competent authorities of the home Member State if the application of such standards is not possible due to the laws of the third country.[39] The shared information concerns information on suspicions that funds are the proceeds of criminal activity or are considered to be related to terrorist financing and as such have been reported to the FIU.

2.3.3 Ultimate Beneficiary Owner Registers

In the European Union, the 4th AMLD obliges European Member States to establish central Ultimate Beneficial Owner (UBO) Registers[40] and provide timely and unrestricted access to information stored in it, in all cases, to competent authorities and FIUs, as well as to obliged entities for the purpose of performing CDD obligations. The UBO Registers consolidate information about the beneficial owners who are defined as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement"[41]. The 4AMLD purported that access to beneficial ownership information should be granted to other persons who are able to demonstrate a legitimate interest. The 5AMLD introduced an important change with regard to the last point. In accordance with the amended Article 30(5) of 4AMLD, Member States should ensure that the information on corporate or other legal entities is accessible not only to a person or an organisation that can demonstrate a legitimate interest, but to the general public. Members of the general public shall be permitted to access at least the following information: the name,

---

[37] Directive 2015/849 (4AMLD), Art. 45(1).
[38] Directive 2015/849 (4AMLD), Art. 3 indent 15.
[39] Directive 2015/849 (4AMLD), Recital 48. On this point see European Banking Authority, European Securities and Markets Authority and Joint committee of the European supervisory authorities, Final Report on Draft Joint Regulatory Technical Standards on the measures credit institutions and financial institutions shall take to mitigate the risk of money laundering and terrorist financing where a third country's law does not permit the application of group-wide policies and procedures, 12.2017, available at https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/rts-on-the-implementation-of-group-wide-aml/cft-policies-in-third-countries. These Regulatory Technical Standards (RTS) will specify how credit and financial institutions should manage money laundering and terrorist financing (ML/TF) risks where a third country's law prevents the implementation in their branches or majority-owned subsidiaries of group-wide policies and procedures on anti-money laundering and countering the financing of terrorism (AML/CFT).
[40] Directive 2015/849 (4AMLD), Art. 30(3).
[41] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2020), p. 117 < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 25 May 2021

the month and year of birth, the country of residence, the nationality of the beneficial owner and the nature and extent of the beneficial interest held.[42]

The EDPS expressed his reservations on the offering of access to the UBO Registers to the public and recommended "[d]esigned access to beneficial ownership information in compliance with the principle of proportionality, inter alia, ensuring access only to entities who are in charge of enforcing the law".[43] However that proposal was not take up by the EU legislative bodies when enacting the 5AMLD.

In the beginning of 2021, the Luxembourg District Court, submitted a referral to the Court of Justice of the European Union (CJEU) requesting a preliminary ruling on the access of the general public to the UBO Registers.[44] Among others, the Luxembourg District Court asked in essence whether the making of information on beneficial owners accessible to the general public without any requirement for legitimate interest to be shown is in line with the rights to privacy and data protection and a number of concrete data protection principles and requirements established in the GDPR. It further asked clarification on the access restrictions which are foreseen for exceptional circumstances.

In the Netherlands, the Dutch NGO Privacy First Dutch filed legal action challenging the Dutch UBO register on data protection grounds, in particular as not respecting the proportionality principle. The Hague District Court did not grant the requested deactivation of the UBO register and Privacy First filed an urgent appeal against the entire judgment of the District Court of the Hague, requesting among others the Court of Appeal of the Hague to submit a request for preliminary ruling to the CJEU, following the example of the Luxembourg case mentioned above.

Attention should be paid to the fact that Directive 2019/1153[45] establishes centralised bank account registries, which are the centralised automated mechanisms, such as central registries or central electronic data retrieval systems, put in place in accordance with Article 32a(1) 4AMLD, as amended by 5AMLD. However, these centralised bank account registers (aiming at facilitating authorities to quickly find out where somebody has accounts so that they can then contact the relevant financial institution for more detailed customer data) are completely different registers from the UBO registers and should not be confused with the latter.

2.3.4 Further access to data by the FIUs

Where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, such obliged entity must inform the FIU. All suspicious transactions, including attempted transactions, need to be reported[46] via an STR, which became the primary source of information on potential money laundering or terrorist financing available to the FIU. After the submission of an STR with all supporting information, the obliged entity can still be contacted by an FIU for any additional necessary information concerning the reported event.[47] In addition, following 5AMLD, FIUs can ask for information independently

---

[42] Directive 2015/849 (4AMLD), Art. 30(5).
[43] EDPS, Opinion 1/2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC – Access to beneficial ownership information and data protection implications (2 February 2017) <https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf> accessed 25 May 2021.
[44] Case C-601/20 *SOVIM SA v Luxembourg Business Registers* [2020].
[45] Directive 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.
[46] Directive 2015/849 (4AMLD) Art. 33(1).
[47] Directive 2015/849 (4AMLD) Art. 33(1)(b) as amended by Directive 2018/843 (5AMLD)

of whether the requested entity filed a prior SAR[48]. This is an important change, as the SAR reporting is now no longer a filter that would serve as a precondition for FIUs to access to obliged entity data.

Other crucial sources of information for the FIUs, next to the STRs or SARs, can originate from other existing public databases. Given that the knowledge gained from the STRs/SARs may need to be supplemented FIUs should "have access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly"[49].

The 4AMLD does not, however, clarify what kind of "financial", "administrative" or "law enforcement" information FIUs should have access to, as well as to what extent should these sources of information be made available to the FIUs in practice. This leaves a lot of discretion to the Member States in determining those matters.

2.3.5 Data sharing within PPPs

In addition to the existing patterns of the exchange of information between the obliged entities, FIUs, competent authorities, Public-Private Partnerships (PPPs) foster the exchange of financial information. The origins of the first financial intelligence sharing PPP can be traced back to 2015, when the Joint Money Laundering Intelligence Taskforce (JMLIT) was created in the United Kingdom. Then, at the turn of 2015 and 2016, in Canada, an initiative known as "Project PROTECT" gave rise to the establishment of a unique PPP for targeting human trafficking for the purposes of sexual exploitation by taking account of the money laundering aspect of the crime.[50] In 2017, the Australian Transaction Reports and Analysis Centre (AUSTRAC) launched a PPP for financial intelligence sharing named "Fintel Alliance". In the same year, in Singapore, the AML/CFT Industry Partnership (ACIP) was created and, in Hong Kong, the Fraud and Money Laundering Intelligence Taskforce (FMLIT). Since then, the numbers of PPPs across the globe have been raising.

With some differences in composition and exact manner of functioning, the PPPs are collaborative platforms established primarily with a view of facilitating the collaboration between the banking sector and the government in the fight against financial crime.[51] Thanks to the collective expertise and resources of both sectors, the detection, prevention and disruption of serious financial crime and money laundering threats is envisaged to be enhanced.

The term PPP has evolved over time and in the AML/CFT fields it serves to describe public-private forms of collaboration for strategic and/or tactical information sharing. It means that at the heart of the collaboration between the public and private partners lies intelligence, which can be generated thanks to combining several pieces of information that are scattered between the members of a PPP, who only when putting it together can create a full picture. The picture created by the transaction monitoring can concern either a specific case and thus allow for investigating some suspicious incidents, or regard more general patterns of criminal activity. Thus, one can conclude that a PPP in the AML/CFT field can serve the purpose of supporting investigations by competent authorities or supporting the compliance of obliged entities, or a combination of both.[52] The main purpose of investigative PPPs is for the private sector to contribute to ongoing investigations of competent authorities. The main purpose of compliance PPPs is for the public sector to contribute to the improvement of private sector's

---

[48] Directive 2015/849 (4AMLD) Art 32(9), as modified

[49] Directive 2015/849 (4AMLD) Article 32(4).

[50] FINTRAC, 'Project PROTECT (Public Service Renewal in Action)' <https://www.fintrac-canafe.gc.ca/emplo/psr-eng.pdf> accessed 25 May 2021.

[51] Oldrich Bures, 'Public-Private Partnerships in the Fight against Terrorism?' [2013] 60(4) Crime, Law and Social Change, p. 441.

[52] Benjamin Vogel, Jean-Baptiste Maillart, *National and international anti-money laundering law* (1st edn Insertia 2020), p. 922 ff and 1015ff.

compliance with the AML/CFT measures (especially CDD). Compliance PPPs, focused on the development and sharing of typologies, are likely to have lower demands for the operational intelligence, and be focused primarily on strategic intelligence. Finally, the hybrid PPPs serve a combination of the purposes of investigative and compliance PPPs.

3. Exchange of data in the field of taxation

3.1 US FATCA

The United States were developing their own policies on the exchange of information for tax purposes relying in essence on the cooperation of financial institutions.[53] In 2010, the United States adopted the Hiring Incentives to Restore Employment Act (HIRE Act), which included the Foreign Account Tax Compliance Act (FATCA). FATCA enabled the United States to levy tax, under their own taxation laws, on all accounts held abroad by individuals subject to taxation in the United States[54]. Garbarino summarises the main points of FATCA as follows:

> *FATCA established a basic principle: a foreign financial institution ("FFI") is subject a 30-percent withholding tax on all its income deriving from the U.S. unless it complies with the FATCA reporting duties in respect to information related to "U.S. Persons" who are account-holders of that institution ("FATCA Data"). So FATCA imposes an extensive third-party monitoring and disclosure regime on FFIs wherever located outside the U.S. in an effort to expose their undeclared foreign assets to the U.S. I.R.S. [International Revenue Service]*
>
> *More specifically FATCA introduced unilaterally a complex mechanism of information gathering managed by financial intermediaries based on four components: 1) the identification of the participating FFI, 2) the requirement of reporting by such FFI on certain U.S. and non-U.S. account-holders, 3) the threat of a withholding tax on U.S. sourced payment in case of non-compliance, and 4) the duty by U.S. Persons to specifically report to the I.R.S. their foreign financial assets.*[55]

3.2 Supranational framework for the exchange of data in the field of taxation

In the beginning of the previous decade a number of regulatory and policy documents were adopted that dealt with the exchange of data for administrative and tax purposes. The Global Forum on Transparency and Exchange of Information for Tax Purposes was founded in 2000 and restructured in September 2009, which works under the auspices of the OECD and G20.

The OECD has adopted a number of instruments that facilitate the exchange of data in the field of taxation. In 1988 the Council of Europe and the Organisation for Economic Cooperation and Development (OECD) adopted a joint Convention on Mutual Administrative Assistance in Tax Matters[56], which was amended by the 2010 Protocol. This treaty allows the Parties, the member States of the Council of Europe and the member countries of OECD,

---

[53] Carlo Garbarino, 'The EU Protection of Tax Data Transferred to Third Countries' (2020) Bocconi Legal Studies Research Paper No. 3730009, p.2.

[54] For the issue of accidental Americans, see below section 10.1

[55] Ibid, p.3.

[56] OECD and Council of Europe, *The Multilateral Convention on Mutual Administrative Assistance in Tax matters: Amended by the 2010 Protocol* (OECD Publishing 2011).

to develop extensive administrative co-operation covering all compulsory taxes, including the exchange of information between Parties.

Article 6 of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters (MAC) purports that two or more parties shall automatically exchange any information that is foreseeably relevant for the administration or enforcement of their domestic laws concerning their taxes[57] on the categories of cases and in accordance with procedures that are determined in a mutual agreement. By virtue of this Article, which requires the competent authorities of the parties to the convention to mutually agree on the scope of the automatic exchange of information and the procedure to be followed, the CRS Multilateral Competent Authority Agreement (CRS MCAA) was adopted. The CRS MCAA is a multilateral framework agreement, which specifies the details on the types of information to be exchanges and the time this will be realized.

Alternatively, jurisdictions may rely on bilateral agreements for the exchange of information, such as a double taxation treaty or a tax information exchange agreement.[58] As will be discussed below, CRS exchanges will take place on the basis of the DAC2 Directive, agreements between the EU and third countries and bilateral agreements, such as the UK-CDOT agreements.[59]

The OECD Model Tax Convention on income and on capital[60] provides a means on settling on a uniform basis the most common issues that arise in the field of international juridical double taxation.[61] Article 26 of the OECD Model Tax Convention provides a basis for all forms of information exchange between competent authorities. The competent authorities of the contracting states shall exchange information as is foreseeably relevant to secure the correct application of the provisions of the Convention of the domestic laws of the Contracting states concerning taxes of every kind.[62]

The Global Forum on transparency and exchange of information for tax purposes supports both the exchange of information on request (EOIR) and the automatic exchange of information (AEOI) between tax authorities, as well as the spontaneous exchange of information.[63]

The EOIR, relies on a system of peer reviews on the EOIR, during which the legal and regulatory framework of a jurisdiction and the implementation of the framework in practice are evaluated. The international standard provides for exchange on request of foreseeably relevant information for carrying out the provisions of a tax convention or for the administration or enforcement of the domestic tax laws of a requesting party.

In 2014, the OECD, working with G20 countries, developed the Standard for Automatic Exchange of Financial Account Information in Tax Matters (the AEOI Standard), commonly known as Common Reporting Standard (CRS), which was subsequently endorsed by the Global Forum. The CRS calls on jurisdictions to obtain information from their financial institutions and automatically exchange that information with other jurisdictions on an annual basis. It sets out the financial account information to be exchanged, the financial institutions required to report, the different types of accounts and taxpayers covered, as well as common

---

[57] Ibid, Article 4.
[58] OECD, Automatic Exchange portal – International Framework for the CRS, <https://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/> accessed 25 May 2021.
[59] Ibid.
[60] OECD, *Model Tax Convention on Income and on Capital: Condensed Version* (OECD Publishing 2017)
[61] Ibid, Introduction.
[62] Ibid, Commentary on Article 26 concerning the exchange of information.
[63] OECD, 'Substantial Activities in No or Only Nominal Tax Jurisdictions: Guidance for the Spontaneous Exchange of Information' (2019) <https://www.oecd.org/tax/beps/substantial-activities-in-no-or-only-nominal-tax-jurisdictions-guidance-for-the-spontaneous-exchange-of-information.htm> 25 May 2021.

due diligence procedures to be followed by financial institutions.[64] In principle, the exchanges take place on a reciprocal basis. The CRS contains four parts: (i) A model Competent Authority Agreement (CAA) for the automatic exchange of CRS information; (ii) The Common Reporting Standard; (iii) The Commentaries on the CAA and the CRS; and (iv) The CRS XML Schema User Guide, which is a schema in XML language for the exchange of information. It should be noted that the CRS draws on the intergovernmental approach to implementing FATCA:

> *The Common Reporting Standard, with a view to maximising efficiency and reducing cost for financial institutions, draws extensively on the intergovernmental approach to implementing FATCA. While the intergovernmental approach to FATCA reporting does deviate in certain aspects from the CRS, the differences are driven by the multilateral nature of the CRS system and other US specific aspects, in particular the concept of taxation on the basis of citizenship and the presence of a significant and comprehensive FATCA withholding tax. Given these features, that the intergovernmental approach to FATCA is a pre-existing system with close similarities to the CRS, and the anticipated progress towards widespread participation in the CRS, it is compatible and consistent with the CRS for the United States to not require the look through treatment for investment entities in Non-Participating Jurisdictions.*[65]

Article 22 MAC on secrecy provides for strict requirements of confidentiality and limits the entities to which the information may be disclosed. It stipulates that any information that is protected by a party under the MAC shall be protected in the same manner as information obtained under the domestic law of the party and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying party as required under its domestic law. Article 22 MAC also specifies the purposes for which the information may be used. Section 5 of the CRS MCAA on confidentiality and data safeguards mirrors to a large extent the provisions of Article 22 MAC. In particular as regards confidentiality and data protection Section 5 CRS MCAA purports that "All information exchanged is subject to the confidentiality rules and other safeguards provided for in the Convention, including the provisions limiting the use of the information exchanged and, to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Competent Authority as required under its domestic law and listed in Annex C [of the CRS MCAA]"[66]. It should be thus highlighted that both Article 22 MAC and Section 5 CRS MCAA allow the sending jurisdiction to specify additional jurisdiction-specific requirements on the protection of personal data which must be followed by the receiving jurisdiction. These data protection requirements are further specified by the competent authority in a notification to the Co-ordinating Body Secretariat specifying any eventual safeguards for the protection of personal data (Annex C), in accordance with Section 7(1)(d) CRS MCAA.

Section 5(2) CRS MCAA establishes an obligation for the competent authority to notify the Co-ordinating Body Secretariat immediately of any breach of confidentiality or failure of safeguards and any eventual sanctions and remedial actions consequently imposed. Non-compliance with this obligation (or any other obligation established in the CRS MCAA) entails a right to suspend the exchange of information with immediate effect (Section 7 CRS MCAA).

3.3 European framework for the exchange of data in the field of taxation

At European Union level, the exchange of information for tax purposes at EU and global level has been high in the European agenda in the last ten years. In 2011 the Council adopted

---

[64] OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters* (2nd edn OECD Publishing 2017), p.3.
[65] Ibid, p. 10.
[66] OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters, Model Competent Authority Agreement and Common Reporting Standard*, Section 5 (2nd edn OECD Publishing 2017).

Directive 2011/16 on administrative cooperation in the field of taxation[67], commonly known as DAC1. DAC1 defines 'automatic exchange' as "the systematic communication of predefined information to another Member State, without prior request, at pre-established regular intervals. In the context of Article 8 [Scope and conditions of mandatory automatic exchange of information], available information refers to information in the tax files of the Member State communicating the information, which is retrievable in accordance with the procedures for gathering and processing information in that Member State".[68]

DAC1 foresees three forms, in which information could be exchanged, i.e. upon a request (the requested authority should communicate any relevant information that it has in its possession or that it obtains as a result of administrative enquiries to the requesting authority); spontaneously (via non-systematic communication, at any moment and without prior request, of information to another Member State); and automatically (when the systematic communication of predefined information to another Member State takes place, without prior request, at pre-established regular intervals). The most relevant article for the topic examined in this report is Article 8 on the scope and conditions of mandatory automatic exchange of information.

Directive 2014/107 (DAC2) modified DAC1 and provided for the automatic exchange of financial account information in Art. 8, para 3a.[69] The CRS, discussed in the previous section, applies in Europe by virtue of the DAC2. The EU legal framework on Administrative Cooperation was complemented with Directive 2015/2376[70] (DAC3) which added to DAC1 Article 8a on the scope and conditions of mandatory automatic exchange of information on advance cross-border rulings and advance pricing arrangements.

Into facilitate the fight against AML/CFT, the Council adopted Directive 2016/2258 (DAC5) as regards access to AML/CFT information by tax authorities.[71] Directive 2016/2258 provides basis for the tax authorities to access the AML information, procedures, documents and mechanisms for the performance of their duties in monitoring the proper application of Directive 2011/16/EU and for the functioning of all forms of administrative cooperation provided for in that Directive.[72] Finally, Directive 2018/822[73] (DAC6) was adopted on the automatic exchange of reportable cross border arrangements.[74] DAC6 obliges intermediaries (such as tax advisors, accountants, law firms and banks) to report certain information on cross-border arrangements to the local tax authorities. It applies to arrangements involving parties in multiple countries, of which at least one is an EU member state.[75]

Figure 2 provides an overview of the Directives on Administrative Cooperation and the major changes they introduced to DAC1.

---

[67] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.
[68] Ibid, Art. 3(9).
[69] Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation.
[70] Council Directive (EU) 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation.
[71] Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities.
[72] Ibid, Art. 22, para 1a.
[73] Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements.
[74] Ibid, Art. 8ab.
[75] ING, 'DAC6: EU Directive against aggressive tax arrangements' <https://www.ing.com/About-us/Compliance/Automatic-Exchange-of-Information-AEOI/DAC6.htm> accessed 25 May 2021.

Figure 2 EU Directives on Administrative Cooperation (DAC)[76]

In 2019 Directive 2019/1153 was adopted, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.[77] This Directive is also of importance to the AML/CFT field, as discussed in section 2.1..

3.4 Exchanges of data for tax purposes

The previous sections made clear that the legal and regulatory framework on inter-state exchange of information regulates mainly the exchange of information taking place between competent authorities. In the context of this report the focus in the field of taxation is on the automatic exchange of information, as these are not only in the focus on the OECD and national legislators, but also because they cover the lion's share when it comes to inter-state exchange of information.

[76] European Commission, 'Administrative cooperation in (direct) taxation in the EU – EU Directives on Administrative Cooperation (DAC)' <https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en> accessed 25 May 2021.

[77] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.

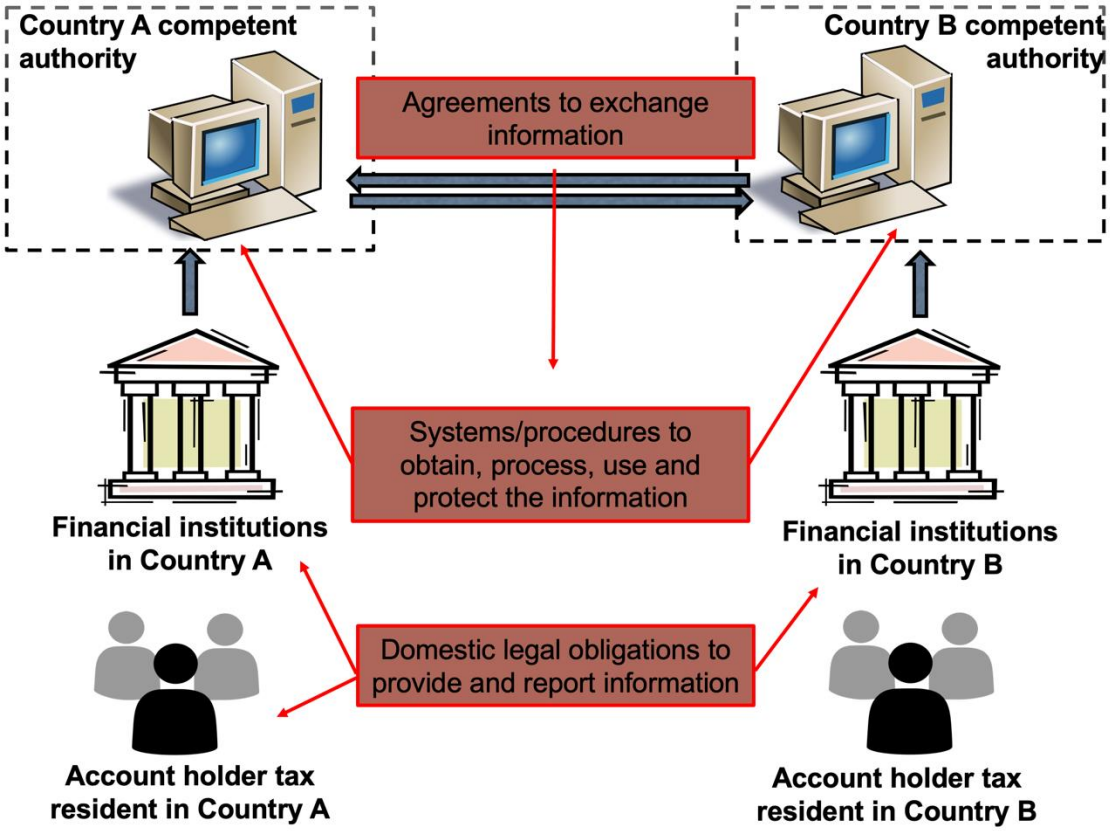

Figure 3 CRS basic framework[78]

4. Actors involved

Convention 108+ recognises four main categories of actors, namely: data subjects, data controllers, data processors, and supervisory authorities. The correct allocation of roles to the actors involved in data processing is pivotal in assigning the corresponding rights and obligations to the relevant actors. In the sphere of both AML/CFT and taxation there are areas of uncertainty as to exactly which categories of persons are concerned and this issue is aggravated when automatic exchanges of personal data take place. The distinction between data subjects, controllers, and processors allows for providing separation of their roles and responsibilities. While the data subjects are equipped with a set rights, a respective set of obligations is imposed on controllers and processors. The supervisory authorities, in turn, are responsible for the enforcement of compliance with the data protection legal framework and facilitation of its effectiveness.

4.1 AML/CFT context

[78] South African Revenue Service, 'How does CRS reporting work' <https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/how-does-crs-reporting-work/> (Figure modified by the author).

In the AML/CFT context, identification and verification of identity is one of the most pivotal CDD measure and a cornerstone of the AML/CFT strategy. This means that the primary data subjects in the AML/CFT context are the customers, which are natural or legal entities, trusts and similar structures (in case of the latter, the ultimate beneficial owners). As far as the natural persons are concerned, there should be no doubt that they are (already) identified or identifiable individuals, and thus certainly data subjects. As regards legal persons, in principle, corporate data in itself are not personal data, unless they are data about an individual. This can be the case of one-person-owned corporations – i.e. entities, where it is impossible to view the corporation and the owner separately, for instance, when the company name is simultaneously the name of the owner. However, the Parties to Convention 108+ "may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate interests".[79]

As regards trusts (and equivalents), the definition of beneficial owner is broader than in case of corporate entities. Consequently, almost every relevant person can qualify as an ultimate beneficial owner, i.e. the settlor, the trustee(s), the protector (if any), the beneficiaries, or any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.[80] The identification of ultimate beneficial owners is essential in order to correctly identify the data subjects in the exchange of data.

More complicated is the allocation of roles of data controllers and data processors to the involved entities. Obliged entities and FIUs are the main relevant actors in this context, while third parties performing CDD measures are also involved.

The obliged entities seem to best fit under the definition of data controllers. They are legal entities that have decision-making power with respect to data processing.[81]The controllership can be defined by law.[82] Obliged entities can outsource the performance of the CDD measures to third parties.[83] From the data protection point of view, the question is whether such entities should be considered data controllers or processors. The decisive factor appears to relate to who has decision-making power with respect to the data processing at issue. Yet, the question is which is the processing at issue. Considering that it is the processing that aims at compliance with the CDD measures by the obliged entity, the third party can be regarded as acting on behalf of that obliged entity and therefore be a data processor. If the third party processes the same sets of data, but for other purposes than those determined in the processing instructions by the data controller, obtaining in this way decision-making power, then for that processing activity, such a third party would be considered as data controller.

---

[79] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) para. 30 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 25 May 2021.

[80] Directive 2015/849 (4AMLD), Art. 3 indent 6 (ii).

[81] Council of Europe, Modernised Convention for the protection of individuals with regard to the processing of personal data ETS No.108, Art. 2(d).

[82] Contribution from the European Data Protection Supervisor, Europol Joint Parliamentary Scrutiny Group - 7th meeting, 28 September 2020, para 19 https://www.europarl.europa.eu/cmsdata/211695/EDPS_letter_23092020.pdf accessed 26 May 2021.

[83] European Banking Authority, EBA report on the future AML/CFT framework int eh EU – Response to the European Commission's call for advice on defining the scope of application and the enacting terms of a regulation to be ado[ted om the field of preventing money laundering and terrorist financing, EBA/REP/2020/25, available at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/931093/EBA%20Report%20on%20the%20future%20of%20AML%20CFT%20framework%20in%20the%20EU.pdf p. 12.

The attribution of either data controllers' or processors' roles in case of processing by a group of undertakings, which can consist of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries participate, poses a difficult task. Following the reasoning of the EDPB, the most crucial is to take into account the factual relationship between the stakeholders involved in the processing. In case of groups, multiple scenarios seem possible. Given that the members of the group are closely connected by organizationally separate entities, each of them can be an independent data controller insofar as it has decision-making power with respect to the data processing. The AML/CFT regimes foresees however the possibility of sharing information, including personal data within a group. In such a case, a joint-controllership can be considered. This requires however, all the controllers, i.e. all members of the group involved in the same processing activity to have decision-making power with respect to data processing. If this is the case, the group can be considered joint-controllers.

The FIUs collect and analyse information with a rather clear aim of identifying grounds to suspect money laundering, associated predicate offences or terrorist financing[84] and later disseminating relevant analyses and information to the competent authorities. Such purpose of processing is determined by the law, which means that the controllership may in fact defined by law[85], giving them decision making power. The legislator designates FIUs as controllers due to their genuine ability to exercise control.[86] The 4AMLD provides only for the competences of FIUs for accessing information from various sources. The details about the collection of information, as well as of the analysis need to be determined by every FIU.

Major concerns arise with regard to the allocation of data protection roles to the entities involved in a PPP for AML/CFT, mainly due to the *de facto* lack of transparency of the arrangements governing the PPP (see section 2.3.5). Given the various structure that such PPPs may have and the various goals they main pursue, there is no one-size-fits-all model that can be applied for the protection of personal data when these are exchanges between the entities involved in the PPP. The analysis shall always take place on a case-by-case basis. It is advisable that when PPPs are established, there is a clear allocation of the roles to the entities that participate in it and a delineation of the rights and obligations in relation to the processing of personal data.

4.2 Field of taxation

The precise definition of the data subjects, whose data are involved in the exchange of information is crucial in order to avoid bulk collection and transfer of personal data. The competent authorities that have the decision-making power with respect to the exchange of the data are the data controllers. However, the role of the entities that are authorized to use the exchanged data will be defined depending on their powers, and in particular whether they have decision making powers. Parties to the Convention shall make sure to include a clear allocation of data protection roles, that bring along concrete rights and obligations, when establishing rules that involve the exchange of data.

5. Sensitive data

Article 6 of Convention 108+ permits the processing of sensitive data only when appropriate safeguards are enshrined in law, complementing the safeguards of the Convention. Sensitive

---

[84] Directive 2015/849 (4ALMD), Article 32.

[85] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 02 September 2020, para 19 <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf> accessed 26 May 2021

[86] Ibid, para. 21.

data are considered the following: “genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life”.

5.1 Processing sensitive data in AML/CFT

In the context of AML/CTF personal data relating to criminal proceedings and convictions are often processed. Thus, in line with Article 6(1) Convention 108+, the processing of personal data relating to criminal proceedings and convictions shall be allowed for AML/CFT purposes only when appropriate safeguards are established in law. At a European Union level the EDPB proposed as such safeguards the following: “it could be provided that obliged entities should only be allowed to process criminal convictions and offences related to money laundering and terrorist financing handed down in countries where the rule of law, and especially the presumption of innocence, the right of defence and right of a fair trial are respected. Another appropriate safeguard could be to ensure the training and expertise of staff that deal with sensitive personal data in the context of AML-CFT obligations. All safeguards should be accompanied by serious corrective measures, including penalties, for the controller (obliged entity or FIU as the case may be) in case of non-compliance”[87].

6. Rights of data subjects

Convention 108+ establishes a number of rights for the data subjects in Article 9, namely:

- the right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration (Article 9(1)(a) CoE Convention 108+), unless such a decision is authorised by law, establishing suitable measures to safeguard the data subject’s rights (Article 9(2) CoE Convention 108+)
- the right to obtain on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her (Article 9(1)(b) CoE Convention 108+)
- the right to receive communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8(1) CoE Convention 108+ that specifies the minimum information to be provided (Article 9(1)(b) CoE Convention 108+)
- the right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her (Article 9(1)(c) CoE Convention 108+)
- the right to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms (Article 9(1)(d) CoE Convention 108+)
- the right to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been,

[87] European Data Protection Board, Letter to the European Commissioner for Financial services, financial stability and Capital Markets Union and to the European Commissioner for Justice (19.05.2021) < https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf> accessed 30 June 2021.

processed contrary to the provisions of this Convention (Article 9(1)(e) CoE Convention 108+)

- the right to have a remedy where his or her rights under CoE Convention 108+ have been violated (Article 9(1)(f) CoE Convention 108+)
- the right to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority, in exercising his or her rights under CoE Convention 108+ (Article 9(1)(g) CoE Convention 108+)

Every Party to CoE Convention 108+ shall assist any data subject, whatever his or her nationality or residence, to exercise their aforementioned rights (Article 18(1) CoE Convention 108+).

6.1 Restrictions under the CoE 108+

Several of the aforementioned rights may be difficult to satisfy when there are overriding interests to be served. For this reason, CoE Convention 108 foresees a number of cases when the rights of data subject can be restricted, some of which can be relevant for the restriction of data subject rights when exchange of personal data takes place for AML/CFT or tax purposes.

Article 11 Convention 108+ allows exceptions to the provisions of of Article 5(4) (data protection principles), Article 7(2) (data breach notification), Article 8(1) (transparency of processing) and Article 9 (data subject rights), when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for the following reasons:

a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.[88]

Additional exceptions may be allowed with regard to processing activities for national security and defense purposes, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, to Article 4(3) (evaluation of effectiveness of measures by the Convention Committee), Article 14(5) and (6) (information to the supervisory authority on data transfers) and Article 15(2)(a),(b),(c) and (d).

6.2 Restrictions under Article 23 GDPR

Article 23 GDPR grants the possibility to restrict the rights attributed to data subjects and the application of all (except for the accountability) basic principles of the processing of personal data. i.e. the rights established in “Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22”, to the extent that these principles relate to the aforementioned rights and obligations. Given that the fundamental right to data protection cannot be ensured without respecting data subject’s rights and adhering to the principles of processing by data controllers, it is crucial

[88] Council of Europe, Modernised Convention for the protection of individuals with regard to the processing of personal data ETS No.108, Article 11(1).

to emphasise that restrictions under Article 23 must be considered exceptions. These exceptions from the general rules can therefore be applied narrowly and only under specifically prescribed circumstances.[89]

Accordingly, Article 23 GDPR requires that the restrictions may be introduced "**by way of a legislative measure**", they must **respect "the essence of the fundamental rights and freedoms", and constitute "a necessary and proportionate measure in a democratic society"** to safeguard one of the following objectives:

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

f) the protection of judicial independence and judicial proceedings;

g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i) the protection of the data subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

The formulation of Article 23 GDPR resembles the one used in Article 52(1) CFR with the differences of referring explicitly to a "legislative measure", relating the requirements of necessity and proportionality to a democratic society (as it is in Article 8(2) ECHR) and providing an exhaustive list of objectives in the pursue of which, the legislator can establish a restriction.

6.3 Restrictions of rights when data are exchanged for AML/CFT and tax purposes.

When personal data are exchanged for AML/CFT and tax purposes, the rights of the data subject may be restricted in three main cases: (a) in the name of prevention, investigation and prosecution of crime, (b) in the name of national security or (c) in the name of other important objectives of general public interest.

[89] EDPB, 'Guidelines 10/2020 on Restrictions under Article 23 GDPR' (December 15, 2020) para. 3 <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf> accessed 25 May 2021.

6.3.1 Restrictions in the name of prevention, investigation and prosecution of criminal offences

While CoE Convention 108+ allows Restrictions in the name of prevention, investigation, and prosecution of criminal offences, Article 23 of the GDPR allows such restriction also for the detection of such criminal offences. The EDPB recently issues guidelines on the interpretation of Article 23.[90] It recognised that in some cases, such as for instance in the framework AML/CFT, the provision of information to the data subjects that are under investigation may jeopardise the investigation itself.[91] However, the data subjects shall be notified when the notification will not jeopardise any more the investigation (see section 5.4 below).

6.3.2 Restrictions in the name of national security

Article 4(2) of the TEU explicitly provides for that national security remains the sole responsibility of each Member State.[92] The European Court of Human Rights (ECtHR) has dealt with restrictions established in the name of national security, it has never defined the scope of the term national security. In a similar vein the CJEU does not provide a definition of national security. In *Esbester* the European Commission for Human Rights (ECmHR) stated that "the term 'national security' is not amenable to exhaustive definition and [considers it satisfactory when] sufficient indication is given of the scope and manner of exercise of the functions of the Security Service. (…)."[93] In *Liberty*[94] the Court relied on the definition of national security given by the British Commissioner designated under the British Interception of Communications Act of 1985.[95] In his report of 1986 the Commissioner defined threats to national security as activities: "which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means."[96] Later on, the Court again mentioned this definition in *Kennedy* [97] when indicating how to apply the term regarding secret surveillance activities in the UK. Under the current UK legislation, RIPA does not contain a definition of national security. However, the notion of national security is found to have an expansive definition spanning from "the classic concept of direct threats (whether internal or external) to the safety of the realm but also indirect ones."[98],[99].

6.3.3 Other essential objectives of general public interest

Article 11(1)(b) CoE Convention 108+ allows for restrictions on the rights of data subjects for other essential objectives of general public interest. Article 23(1)(e) of the GDPR, in the corresponding provisions to Article 11(1)(b) GDPR mentioned as other important objectives

---

[90] Ibid.

[91] Ibid, para. 24

[92] Treaty on European Union (Lisbon Treaty) Article 4(2).

[93] *Esbester v United Kingdom* App no 18601/91 (ECtHR, 2 April 1993).

[94] *Liberty and Others v United Kingdom* App no 58243/00 (ECtHR, 1 October 2008), para 20.

[95] The British Interception of Communications Act of 1985 was the predecessor of the UK Regulation of Investigatory Powers Act (RIPA) 2000.

[96] The British Commissioner designated under the British Interception of Communications Act of 1985, Report of the UK Commissioner of 1986 under reference of *Liberty and Others v United Kingdom* App no 58243/00 (ECtHR, 1 October 2008), para 20.

[97] *Kennedy v United Kingdom* App no 26839/05 (18 August 2010), para 159.

[98] Eric Metcalfe, 'Terror, reason and rights' in Esther D. Reed et al. (eds) *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives* (Cambridge University Press 2012) 155.

[99] Eleni Kosta, 'Surveilling Masses and Unveiling Human Rights – Uneasy choices for the Strasbourg Court', Tilburg Law School Research Paper No. 2018-10, p 32.

of general public interest "an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters…".[100]

6.3.4 Safeguards when applying restrictions

In its recent case law, the CJEU has offered some clarifications on the limitations and restrictions established for national security. In *Privacy International*, the CJEU examined national legislation enabling a state authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security. A number of European governments argued in *Privacy International* that "the activities of the [national] security and intelligence agencies are essential State functions relating to the maintenance of law and order and the safeguarding of national security and territorial integrity, and, accordingly, are the sole responsibility of the Member States" and therefore national measures concerning the safeguarding of national security cannot be considered falling within the scope of the e-Privacy Directive.[101]

However, the CJEU argued that, it is apparent from Article 23(1)(d)[102] and 23(1)(h)[103] GDPR that the processing of personal data carried out by individuals for those same purposes falls within the scope of the GDPR.[104] The CJEU concluded that "although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, **the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law**". In simple words, the CJEU clearly found that national measures taken for the purpose of protecting national security cannot render EU law inapplicable as such and exempt the Member States from their obligation to comply with that law[105]. Similar conclusion was reached in the *LQDN* judgment where the CJEU concluded that "national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime … falls within the scope of [European Union legislation; in this case] Directive 2002/58.[106] Following the reasoning of the CJEU, private entities involved in the exchanges of personal data either for tax purposes or -even maybe more prominently- for AML/CFT remain under the scope of the GDPR, even when the exchange has been requested by a competent authority (which could also be an FIU in case of AML/CFT). As such, careful examination of the regime under which the exchange of data is realised, especially when private entities are involved is essential, in order to restrict rights of the data subjects.

---

[100] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), Article 23(1)(e).

[101] Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others [2020] ECLI:EU:C:2020:790, paras 32-33.

[102] GDPR Article 23(1)(d) on the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

[103] GDPR 23(1)(h) on a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) [national security] to (e) and (g).

[104] Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others [2020] ECLI:EU:C:2020:790, para. 47.

[105] Ibid, para. 44.

[106] Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and others v Premier Ministre and others [2020] ECLI:EU:C:2020:791, para. 102.

6.4 Notification of persons concerned

The notification of concerned persons is probably the most prominent right of the affected data subjects that is often at odds with the goals of combating ML/FT and tax fraud/evasion. The AML/CFT framework does not provide for an obligation to inform persons whose transactions were under scrutiny for AML/CFT purposes or were shared with the FIUs or law enforcement authorities, not even when there is no risk of jeopardizing any of the ongoing operations. In fact there is actually a prohibition to notify such persons that may extend even to a non-disclosure within court proceedings. Similarly, the framework on the exchange of data for tax purposes does not contain such an obligation either. However, in both these frameworks, the notification of the data subjects when personal data are exchanged is a right of the relevant data subjects. This right can only be restricted, as described above under specific circumstances and offering concrete safeguards to the data subjects. The ECtHR and the CJEU have provided some guidance on the issue of notification.

It has been established case law of the ECtHR in the context of the interception of communications that the notification of concerned individuals is "inextricably linked to the effectiveness of remedies before the courts"[107] and that the persons concerned should be informed "[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure."[108] This was also repeated in later case law on secrete surveillance: "after the surveillance has been terminated, the question of subsequent notification of surveil-lance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers".[109]

The issue of notification of the affected individuals was crucial in *Tele2/Watson* and the CJEU stated that "the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy".[110] This position as repeated in the CJEU Opinion 1/15 on the EU-Canada PNR agreement.[111]

Although the right of data subjects to be notified when their personal data are processed can be restricted in the framework of combating ML/FT and tax fraud/tax evasion, this shall not be done in a blanket way. Based on the case law of the CJEU and the ECtHR, the relevant authorities may refrain from informing the data subjects about their processing of their personal data. However, these authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations. Supervisory authorities shall have the power to examine whether the notification of the data subjects is actually realised.

The CJEU in *La Quadrature du Net* proposed additional safeguards on the right to notification when there is "automated" analysis of the data. The CJEU argued that when notification is

---

[107] See among others, *Roman Zakharov v. Russia* App no 47143/06 (ECtHR, 4 December 2015), para 234.

[108] *Roman Zakharov v. Russia* App no 47143/06 (ECtHR, 4 December 2015) para 287, with refrence to *Klass and Others v. Germany* App no 5029/71 (ECtHR, 6 September 1978) para 58 and *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006) para 135. Similar reflections were made by the Court in *Szabó and Vissy v. Hungary* App no 37138/14 (ECtHR 12 January 2016) para 86.

[109] *Roman Zakharov v. Russia* App no 47143/06 (ECtHR, 4 December 2015), paras 233-234.

[110] Joined Cases C-2013/15 and C698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson* [2016] ECLI:EU:C:2016:970, para 121

[111] Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraphs 222 and 224 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5512101> accessed 25 May 2021.

required in the context of automated analysis (of traffic and location data, in that given case) "the competent national authority is obliged to publish information of a general nature relating to that analysis without having to notify the persons concerned individually. However, if the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning him or her, it is necessary to notify that person individually. That notification must, however, occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible".[112]

La Quadrature du Net was a case about French authorities that collected traffic and location data. The CJEU established a general obligation for the national competent authorities to publish information of a general nature relating to the automated analysis of the data, without having to notify the persons concerned individually. However, the CJEU established a must stricter obligation when the data matches the parameters specified in the measure authorising automated analysis and that authority identifies the person concerned in order to analyse in greater depth the data concerning these persons. In this cases the CJEU finds it necessary to notify that person individually. In line with its established case law, the CJEU concluded that notification must occur only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those authorities are responsible.

This position of the CJEU is of great importance when automated analysis of data takes place in both the tax fraud/tax evasion context and in the AML/CFT framework. It is unclear whether the CJEU aimed at imposing such an obligation to notify individually the persons concerned when these persons have been singled out based on automated analysis only to national authorities or whether such an obligation should be expanded to private entities as well. This latter concern would have great impact on obliged entities in the AML/CFT framework, which are already making use of AI in order to carry out data mining and profiling operations.

6.5 Reflection on the restrictions of rights in AML/CFT

As, already mentioned above, when personal data are exchanged for AML/CFT, the rights of the data subject may be restricted in three main cases: (a) in the name of prevention, investigation and prosecution of crime, (b) in the name of national security or (c) in the name of other important objectives of general public interest.

It is questionable however which would be the most appropriate ground to justify the restrictions to the rights of the data subjects. The primary aim of the AML/CFT framework is to detect financial transactions that may involve illicit assets or contribute to financing terrorism but not to protect against those per se. Therefore, perhaps it would be more suitable to justify an interference with a view of pursuing other important objective of general public interest of the Union or of a Member State, which in this case, as follows from many recitals to the AML Directive would be the protection of the financial system.

4AMLD establishes a rule for the limitation of the right of access. Article 39 of 4AMLD establishes a general secrecy surrounding the AML/CFT policies and prohibition of disclosure regard STR/FIU requests. Art. 41(4) of the 4AMLD stipulates that "in applying the prohibition of disclosure laid down in Article 39(1), Member States shall adopt legislative measures restricting, in whole or in part, the data subject's **right of access to personal** data relating to him or her to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned to: (a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or (b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes

[112] Ibid, para. 191.

of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardized"[113] (emphasis added).

6.6 Reflection on the restrictions of rights for tax purposes

There is an intrinsic conflict between the rights of data subjects, whose personal data are exchanged, and the goals of the tax fraud/tax evasion system. In the European Union, DAC1 foresees limitations to specific data protection rights of data subjects when their data are exchanged for tax purposes: "All exchange of information pursuant to this Directive shall be subject to the provisions implementing Directive 95/46/EC. However, Member States shall, for the purpose of the correct application of this Directive, restrict the scope of the obligations and rights provided for in Article 10, Article 11(1), Articles 12 and 21 of Directive 95/46/EC to the extent required in order to safeguard the interests referred to in Article 13(1)(e) of that Directive"[114]. Directive 1995/46 (Data Protection Directive) has been replaced by Regulation 2016/679 (General Data Protection Regulation - GDPR) and the references to the Data Protection Directive shall be construed as references to the GDPR.[115] DAC1 obliges ("shall") member states to restrict the right of data subjects to receive information in cases when data are collected from the data subject or from another source and the right of access and shall restrict the publicizing of processing operations. These restrictions shall be made to the extent necessary in order to safeguard important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security.[116]

Recently, the CJEU in *Luxemburg State*, found that Article 47 CFR precludes legislation of a Member State implementing the procedure for the exchange of information on request established by Directive 2011/16 which prevents a person holding information from bringing an action against a decision by which the competent authority of that Member State orders that person to provide it with that information, with a view to following up on a request for exchange of information made by the competent authority of another Member State. Art 47 CFR shall also be interpreted as not precluding such legislation from preventing the taxpayer concerned, in that other Member State, by the investigation giving rise to that request for exchange of information and the third parties concerned by the information in question from bringing actions against that decision.[117] This judgment confirms that tax information exchange does not operate in a parallel universe and that data protection rules and principles apply to any other areas of the law. With regard to the right to an effective remedy, the CJEU interpreted it as requiring that persons who hold information that is requested by the national administration in the context of a cooperation procedure between Member States, must be able to bring a direct action against such a requirement.

7. Legal basis for the exchange of personal data

The principle of lawfulness means that the processing of personal data relies on at least one of the appropriate lawful basis. Article 5(2) of the Convention 108+ purports that data shall be processed "on the basis of the free, specific, informed and unambiguous consent of the

[113] Directive 2015/849 (4AMLD) Art. 41(4).
[114] Directive 2011/16/, Article 25(1).
[115] GDPR Article 94.
[116] GDPR Article 23(1)(e).
[117] Cases C-245/19 and C-246/19 *État luxembourgeois v B and État luxembourgeois v B,C,D,F.C* [2020] ECLI:EU:C:2020:795.

data subject or of some other legitimate basis laid down by law".[118] The explanatory report to Convention 108+[119] clarifies that the notion of 'legitimate basis laid down by law' "encompasses, inter alia, data processing necessary for the fulfilment of a **contract** (or precontractual measures at the request of the data subject) to which the data subject is party; data processing necessary for the protection of the **vital interests** of the data subject or of another person; data processing necessary for compliance with a **legal obligation** to which the controller is subject; and data processing carried out on the basis of grounds of **public interest** or for overriding **legitimate interests** of the controller or of a third party"[120]. Interesting in this context is the clarification in the explanatory report that "[d]ata processing carried out on grounds of **public interest** should be provided for **by law**, inter alia, for **monetary, budgetary and taxation** matters, public health and social security, the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, the protection of national security, defence, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the enforcement of civil law claims and the protection of judicial independence and judicial proceedings"[121].

7.1 Exchanges of data for tax purposes

The exchange of personal data for tax purposes relies usually on the ground that the processing of data is necessary for the compliance with a legal obligation to which the controller is subject. The main legal basis for the exchange of personal data for tax purposes is usually a bilateral convention on income tax or a multilateral agreement on mutual assistance or exchange of information. Such examples are:

- The joint Council of Europe/OECD Multilateral Convention on Mutual Administrative Assistance in Tax Matters
- Council Directive 2011/16 on administrative cooperation in the field of taxation, as amended
- Council Directive 2018/822 as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements

7.2 Exchanges of data for AML/CFT

The legal basis of the exchange of data is more complicated in the field of AML/CFT, where various actors are involved. As regards the processing by the obliged entities in the pursue of the CDD measures, as regulated in the 4AMLD, one can agree that indeed the GDPR should apply. This is because the GDPR as a general regime applies to any processing operation, unless the conditions for any of the exceptions set out in Article 2(2) and (3) GDPR are met.[122] Considering that the obliged entity is not a competent authority in the meaning of

---

[118] Council of Europe, Modernised Convention for the protection of individuals with regard to the processing of personal data ETS No.108, Article 5(2).

[119] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 25 May 2021.

[120] Ibid, para 46.

[121] Ibid, para 47.

[122] Article 2(2) GDPR excludes application of the GDPR for the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural

LED[123] and does not process personal data for the law enforcement purposes, or at least not directly, as well as that no other exceptions are relevant, the GDPR as *lex generalis* is the applicable regime. The situation may be different with regard to the FIUs. The 4AMLD lays down basic rules for the functioning and tasks of the FIUs. Considering the role of the FIUs in the AML/CFT legal system and character of the FIUs, and particularly those of the law enforcement type, one can argue that not the GDPR, but the LED should be the applicable legal framework.[124] Therefore, it should be concluded that despite the wording of Article 43 of the 4AMLD, the GDPR does not necessarily apply to all data processing operations for the purposes of the prevention of money laundering and terrorist financing that are foreseen in the 4AMLD.

At European Union level, the 4AMLD, as amended by 5AMLD, in Article 43 stipulates that "the processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 **shall be considered to be a matter of public interest under** [the GDPR]".[125] Recital 42 to 4AMLD adds that "[t]he fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States".

When it comes to processing of data carried out by the FIUs, the lawful basis can be 6(1)(c) GDPR, i.e. that the data processing is necessary for compliance with a legal obligation of the FIUs. Alternatively, FIUs can process personal data on the basis on Article 6(1)(e) GDPR, i.e. the processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller, the FIUs in this case. When it comes to the exchange of personal data within a group (with branches and subsidiaries in third countries), this can be realised mainly on the basis of Article 6(1)(c) GDPR, when the processing is necessary for compliance with a legal obligation, when data are exchanged for compliance with CDD obligations for instance. However, Article 43 4AMLD may be interpreted as allowing obliged entities to process more data that those absolutely necessary for compliance with CDD obligations. In these cases, obliged entities could potentially rely on the legitimate interest, either of the obliged entity or of a third party. Obliged entities could process personal data arguing that these are necessary for the performance of a task carried out in the public interest, although this would be accepted in exceptional cisrcumtances. However, the EDPS has argued that "the relevant legitimate ground for the processing of personal data should more appropriately be the necessity to comply with a legal obligation by the obliged entities, competent authorities and FIUs (i.e. Article 7(c) [now 6(1)c)]"[126].

---

person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Article 2(3) GDPR provides for an exception to the processing of personal data by the Union institutions, bodies, offices and agencies.

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

[124] Teresa Quintel, 'Follow the Money, If You Can - Possible Solutions for Enhanced FIU Cooperation Under Improved Data Protection Rules' (2019) University of Luxembourg Law Working Paper No. 001-2019 <https://doi.org/10.2139/ssrn.3318299> accessed 25 May 2021.

[125] Directive 2015/849 (4AMLD), as amended by Directive 2018/843 (5AMLD), Article 43.

[126] See EDPS, Opinion on a Proposal for a Directive of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, and a Proposal for a Regulation of the European Parliament and of the Council on Information on the Payer Accompanying Transfers of Funds (4 July 2013), para. 33 < https://edps.europa.eu/sites/default/files/publication/13-07-04_money_laundering_en.pdf> accessed 25 May 2021.

It is advised that when private entities exchange data for AML/CFT purposes, they clarify the legal basis for this exchange.

8. Data protection principles

Article 5 of COE Convention 108+ stipulates a number of principles for the legitimacy of data processing and the quality of data, which shall be respected whenever personal data are exchanged. The principles established in Article 5(4), i.e. fairness and transparency, purpose limitation, data minimisation, data accuracy and storage limitation, can be restricted in line with Article 11 CoE Convention 108+ (see section 5.1 above).

8.1 Proportionality

Article 5(1) Convention 108+ purports that "[d]ata processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake". In the context of the exchange of personal data, the principle of proportionality shall already be respected at the stage of deciding whether such exchange is necessary or not.[127]

The CJEU applied the proportionality test to the Data Retention Directive[128] in the famous *Digital Rights Ireland* case[129]. The Data Retention Directive obliged Internet Service Providers (ISP) to retain for maximum two years all traffic data of every user in order to share them with the authorities in the context of possible investigations. The Data Retention Directive did not pass the proportionality test. According to the court, the kind of surveillance carried out by Internet Service Providers was particularly intrusive. Despite that, the Data Retention Directive did not provide any safeguard for the protection of the individuals surveilled, which were actually unaware and uninformed of the collection of their traffic data, and of their uses. It also failed to limit the number of people that could have access to said data. Furthermore, the Data Retention Directive was deemed not specific enough in its formulation, due to a lack of connection of the surveillance activities with one or more specific crimes and any lack of evidence of the actual effectiveness of the measure.

In the light of the above, it is reasonable to raise doubts concerning the use of data-driven technologies for AML/CFT.[130] The *Digital Rights Ireland* case present several similarities with the kind of activities carried out in the context of AML/CFT. Data-driven technologies used

---

[127] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) para. 40 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 25 May 2021.

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

[129] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238. See also: Joined Cases C-2013/15 and C698/15 Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson [2016] ECLI:EU:C:2016:970.

[130] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, 'Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647420> accessed 25 May 2021.

for AML/CFT imply a significant intrusion with the fundamental rights of individuals (due to the indiscriminate surveillance and data collection and retention of all bank customers[131]), their also include a risk-assessment, and they do not provide for certain safeguards (individuals are not aware of being flagged by the system and being investigated, there is a lack of procedures to object to the treatment or its results, the software are opaque).

The following points, in particular, appear problematic from the point of view of non-discrimination, based on the principle of proportionality and how it has been applied by the CJEU.[132] While AML/CFT screening activities are supported by the law (the FATF Recommendations, 4AMLD and 5AMLD), it is debatable whether this latter is specific enough; the freedom of manoeuvre left to obliged entities, together with the lack of specific safeguards, might hint in the direction of the law not being specific enough.[133] Recital 43 4AMLD, affirming that the 4AMLD complies with the EU Charter, and Recitals 65 and 66 4AMLD, establishing that Member States must ensure the respect of the right to non-discrimination, appear challenging to apply in practice. Moreover, the lack of transparency, together with the lack of information given to the individuals who are flagged by a software, and the lack of a procedure within obliged entities to object to the procedure/result represent important issues in terms of lack of safeguards for the fundamental rights of individuals. The black box effect can be worsened by the circumstance that the software are usually proprietary technologies and their use within an organization can be protected by trade-secrets. Intellectual Property law might hinder the disclosure of important information about the logic and training of algorithms.

8.2 Fairness and transparency

According to Article 5(4)(a) Convention 108+ "[p]ersonal data undergoing processing shall be processed fairly and in a transparent manner (see also section 6 on the restrictions of the rights of data subjects).

8.3 Purpose limitation

Article 5(4)(b) Convention 108+ requires that personal data undergoing processing shall be "collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes". Purposes should be thus clearly defined and precise and further processing cannot be allowed for purposes that are incompatible to the initial ones.

The principle of purpose limitation is composed of two elements: (1) the data controller must only collect data for specified, explicit and legitimate purposes; and (2) once data are

---

[131] Recital 44 of the AMLD4 establishes, to avoid a ripple effect of the *Digital Rights Ireland* decision, that the retention should be longer than five years, and that appropriate safeguards need to be in place. It is not clear whether this formulation is specific enough.

[132] Gloria González Fuster, Serge Gutwirth and Erika Ellyne, 'Profiling in the European Union: A high-risk practice' (2010) INEX Policy Brief no. 10 <http://aei.pitt.edu/14984/1/INEX_PB10_Fuster_et_al._on_Profiling_in_the_EU_e-version.pdf> Accessed 25 May 2021

[133] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, 'Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?', 17 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647420> accessed 25 May 2021.

collected, they must not be further processed in a way incompatible with those purposes. The first element calls for establishing the purpose clearly. The availability of a specific and explicit purpose is the first requirement of the purpose limitation principle, followed by the ensuring the legitimacy of that purpose. The second element concerns the so-called further processing, i.e. the processing for a different purpose than the one for which data was initially collected. Such a processing can only take place on condition that it is not "incompatible" with the initial purpose.

The explanatory report to the Convention 108+ clarified some criteria that can be used when assessing whether further processing can be considered as compatible to the initial purposes: "In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data is initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia, any link between those purposes and the purposes of the intended further processing; the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to its further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations".[134] Legislators shall be urged to define concretely the purposes for which the exchange of information is required, in order to avoid exchanges of data for other purposes which may well be legitimate, but are not compatible with the initial ones.

8.3.1 Exchanges of data for tax purposes

As regards the purpose limitation principle, while some of the signatory States to the Convention stipulate in their domestic law that automatic processing may be carried out for several different purposes, others have opted for the principle of unity of purpose. It should become clear that in any case, when personal data are exchanged, the purpose limitation principle should be clearly respected.

Purpose limitation is a major point of concern in the field of exchange of data for tax purposes, as often competent authorities would like to use available information for other purposes as well, if they consider it useful. There are still cases where the purposes for which personal data are exchanged are not always clearly specified, leaving room for exchanges of data that would not be in line with the data protection requirements. This is nevertheless gradually changing, as can be illustrated by the example of the Dutch Tax Authority, which has been twice already the subject of investigation by the Dutch Data Protection Authority, which has resulted in strict compliance with data protection regulations, requiring for instance a clear legal basis for the processing to be lawful.[135]

Article 26 of the OECD Model Tax Convention, as updated, is a clear illustration of such a case: "Notwithstanding the foregoing, information received by a Contracting State may be used for other purposes when such information may be used for such other purposes under the laws of both States and the competent authority of the supplying State authorises such use"[136]. The justification for this amendment to Article 26 of the OECD Model Tax Convention

---

[134] Council of Europe, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (2018) para. 49 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> accessed 25 May 2021.

[135] AKD Benelux lawyers, Unlimited information exchange by the Dutch tax authority - GDPR-proof?, July 2019, available at https://www.akd.eu/insights/unlimited-information-exchange-by-the-dutch-tax-authority-gdpr-proof-

[136] OECD, Update to Article 26 of the OECD Model Tax Convention and its Commentary, Approved by the OECD Council on 17 July 2012, <https://www.oecd.org/ctp/exchange-of-tax-information/120718_Article%2026-ENG_no%20cover%20(2).pdf> accessed 25 May 2021.

was it took "into account recent developments and to further elaborate on the interpretation of certain provisions of this Article. Paragraph 2 of the Article was amended to allow the competent authorities to use information received for other purposes provided such use is allowed under the laws of both States and the competent authority of the supplying State authorises such use"[137]. The important element in this amendment is that the further use "shall be allowed under the laws of both states and the competent authority of the supplying State authorises such use". The fact that the competent authority has to authorise the further use of the data is important because it allows the competent authority to assess and decide whether the new purpose is compatible with the original purpose. In addition, it is an opportunity for the competent authority that supplied the information to consult the data protection authority about the proportionality of the further processing. In any case, a strict assessment of the compatibility for further processing should be conducted in compliance with the data protection rules.

There are cases when further processing does not require authorisation. For example, transfers of data to competent Courts do not require such an authorisation, while a notification to the tax authority should still be required.

8.3.2 Exchanges of data for AML/CFT

FATF Recommendation 3 on the definition of money laundering offence requires that "Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences". The interpretative note to Recommendation 3 clarifies that "2…Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches. 3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment"[138]. FATF Recommendation 3 shall be read in a restricted way in respect of the purpose limitation principle, ensuring that all proceedings are intrinsically linked to AML/CFT offences.

The 4AMLD contains a clear provision on purpose limitation in Article 41(2): "Personal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited".

The EDPS has identified a danger for the purpose limitation principle that can potentially arise in relation to PPPs created for the sharing of operational information on intelligence suspects. The EDPS is concerned that "[i]n particular, obliged entities participating in PPPs might be tempted to integrate the information shared by law enforcement authorities through this platform **in their global databases, so as to re-use it later,** as part of their customer profiles. This could lead to discrimination against certain clients, for instance, those offering low profitability for the bank and presenting a significant level of risk, conceivably resulting in the financial exclusion of vulnerable individuals and communities (the so-called "de-risking"

---

[137] Ibid, para 4.3.

[138] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2020) interpretive note to recommendation 3, pp. 38-39 < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 25 May 2021.

of financial entities whereby relationships with clients that may pose risks are terminated or restricted)."[139]

8.4 Data minimization

Article 5(4)(c) Convention 108+ establishes the data minimisation principle, according to which personal data undergoing processing shall be "adequate, relevant and not excessive in relation to the purposes for which they are processed".[140] The entities sending the data must be able to justify, in each case of sharing of personal data, why the specific data were needed for the specific purpose. The legislation, wherever possible, shall be as concrete as possible regarding the data that can be collected by an entity and the data that can be shared for specific purposes.

8.4.1 Exchanges of data for tax purposes

As already mentioned in the introduction, Article 26 of the OECD Model Tax Convention provides a basis for all forms of information exchange between competent authorities, establishing that "[t]he competent authorities of the Contracting States shall exchange such information as is foreseeably relevant for carrying out the provisions of this Convention or to the administration or enforcement of the domestic laws concerning taxes of every kind and description imposed on behalf of the Contracting States, or of their political subdivisions or local authorities, insofar as the taxation thereunder is not contrary to the Convention"[141].

The standard of "foreseeable relevance", mentioned in Article 26 of the OECD Model Tax Convention, is intended to provide for exchange of information in tax matters to the **widest possible extent** and, at the same time, to clarify that Contracting States are not at liberty to engage in "fishing expeditions" or to request information that is unlikely to be relevant to the tax affairs of a given taxpayer"[142] (emphasis added). It is doubtful whether the data minimisation principle can be respected in cases when the exchanged information that is "foreseeably relevant" for the purpose for which the data are exchanged. States shall ensure that the data minimisation is respected and that the competent tax authorities will be balancing the requested data to be exchanged with the purposes that need to be achieved.

8.5 Accuracy

Article 5(4)(d) Convention 108+ requires personal data undergoing processing to be "accurate and, where necessary, kept up to date".[143]

---

[139] EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (23 July 2020), para. 46 <https://edps.europa.eu/sites/default/files/publication/20-07-23_edps_aml_opinion_en.pdf> accessed 25 May 2021.

[140] Council of Europe, *Modernised Convention for the protection of individuals with regard to the processing of personal data* ETS No.108, Article 5(4)(c).

[141] OECD, *Model Tax Convention on Income and on Capital: Condensed Version* (OECD Publishing 2017), Art.26(1).

[142] OECD, Update to Article 26 of the OECD Model Tax Convention and its Commentary, Approved by the OECD Council on 17 July 2012, <https://www.oecd.org/ctp/exchange-of-tax-information/120718_Article%2026-ENG_no%20cover%20(2).pdf> accessed 25 May 2021.

[143] Council of Europe, *Modernised Convention for the protection of individuals with regard to the processing of personal data* ETS No.108, Article 5(4)(d).

8.5.1 Exchange of data in AML/CFT

The accuracy of the data is essential not only for the compliance with data protection, but also for the effectiveness of the AML/CFT, as recognised by the EDPB in the context of the upcoming revision of the European AML/CFT framework.[144] The EDPB has raised a very important issues relating to the accuracy of the data, that is relevant for all countries within and outside the European Union: "obliged entities are increasingly dependent on external sources known as "watchlists", which are provided by third parties. These "watchlists" are commonly used by obliged entities to screen their databases and verify relevant information about their clients, in order to fulfil their legal obligations, and notably to assess the risk of the business relationship. The providers of these "watchlists" are in general controllers under the GDPR and do not fall under the current AML- CFT legislation. Nevertheless, the data processing performed in the context of these watchlists raise serious concerns, considering the quantity and sensitive nature of personal data they process which could lead to serious damage to the rights and freedoms of data subjects. Moreover, the fact that obliged entities make use of these databases provided by third parties does not exempt them from ensuring the accuracy of personal data that they process. The EDPB therefore recommends to seize to create a specific legal framework for "watchlists" and, in particular, to clarify the responsibilities between obliged entities and the watchlists providers regarding GDPR obligations, to provide guarantees especially regarding the compilation of sensitive data, as well as to regulate the consultation of those lists by obliged entities and specify how data subject rights are respected in this context"[145]. Similar recommendations can be made for all CoE contracting parties to ensure the accuracy of the data, especially, when these are obtained from a "watchlist|" such as for instance from social media.

The EDPS highlighted that the European Commission Communication on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing[146] points out "the lack of regulation on exchanges of information between Member States' FIUs and FIUs of third countries which has led to a non-harmonised approach to such exchanges. **These legal and practical obstacles inevitably have an impact on the accuracy and up-to-date information of FIU.net** and thus constitute a risk for the protection of the rights to privacy and personal data."[147]

In order to build an accurate customer profile, obliged entities derive valuable information from the customer behavior with the assistance of Machine Learning and Data Mining techniques.[148] In the case of rule-based software, the accuracy issues are mainly connected to the very rule-based mechanism, that can lead to over-inclusiveness. For instance, less sophisticated rule-based software might flag every transaction over a certain threshold, or

---

[144] European Data Protection Board, Letter to the European Commissioner for Financial services, financial stability and Capital Markets Union and to the European Commissioner for Justice (19.05.2021) < https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf> accessed 30 June 2021.

[145] European Data Protection Board, Letter to the European Commissioner for Financial services, financial stability and Capital Markets Union and to the European Commissioner for Justice (19.05.2021) < https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf> accessed 30 June 2021.

[146] European Commission, Communication of 7 May 2020 on an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, C(2020)2800 final (the "Action Plan") <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:C(2020)2800&from=EN> accessed 25 May 2021.

[147] EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (23 July 2020), para. 31 <https://edps.europa.eu/sites/default/files/publication/20-07-23_edps_aml_opinion_en.pdf> accessed 25 May 2021

[148] Hossein Hassani, Xu Huang and Emmanuel Silva, 'Digitalisation and Big Data Mining in Banking' (2018) 2 Big Data and Cognitive Computing 18.

potential customers because of their country of origin. This generates a very high number of alerts, of which usually only between 1 and 10% refers to actual suspicious cases.[149] This high number of alerts has to be verified with limited personnel and time, creating a bottleneck effect.[150] Furthermore, due to the rigidity of the rule-based system, it can be easier for organized crime to create networks of false names, companies, and chain-transactions that go undetected by the software.

In the case of Machine Learning software, the accuracy of its outputs depends significantly on the completeness and quality of the input, that is, on the data used to assess a prospective customer or a transaction. In addition to the data, the accuracy of the output also depends on how the software has been trained and what kind of patterns and correlations it has detected: if the software presents biases or inaccurate correlations, the predictions it makes might not be reliable.

8.6 Storage limitation

Data shall also be "preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed".[151] It is crucial in order for the storage limitation principle to be respected that the legislation clearly mentions the retention periods during which data shall be retained after their exchange. The determination of the retention period shall respect the proportionality principle. The EDPB has criticised for instance that the retention periods proposed in AMLD4 are too long: "The retention period is the business relationship plus five years (article 40 of Directive (EU) 2015/849). Where the business relationship only covers a single transaction, the retention period is five years. Where there is a long-term business relationship, such as a bank has with its customers, the retention period will often extend over several decennia. Retention periods can be extended by Member States with an additional five years"[152].

9. Data security

Article 7 CoE Convention 108+ requires Parties to the Convention shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. Similar obligations, although more elaborate, are established in Article 32 GDPR. When personal data are exchanged, the recipients of the data shall be clearly identified and appropriate measures shall be put in place in order to allow access to the data only to these specified recipients.

---

[149] Arin Ray, 'DAWN OF A NEW ERA IN AML TECHNOLOGY' (2018); Antoinette Verhage, 'Between the Hammer and the Anvil? The Anti-Money Laundering-Complex and Its Interactions with the Compliance Industry' (2009) 52 Crime, Law and Social Change 9.

[150] Araliya Samme, 'Automated Financial Crime Technology Can Fix the Bottleneck of AML Transaction Monitoring' (*Featurespace*) <https://www.featurespace.com/newsroom/automated-financial-crime-technology-can-fix-the-bottleneck-of-aml-transaction-monitoring/> accessed 26 May 2021.

[151] Council of Europe, *Modernised Convention for the protection of individuals with regard to the processing of personal data* ETS No.108, Article 5(4)(e).

[152] European Data Protection Board, Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing (15.12.2020) < https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf> accessed 30 June 2021.

Compliance with the principle of data security requires the encryption of the data and rules on the full traceability of the exchanges, especially through the implementation of access logs.[153]

10. Transborder flows of personal data

Given the multilateral nature of mechanisms for inter-state exchanges of personal data for tax and AML/CFT purposes, the question of adequate protection arises in all cases where the exchange of personal data involves a country that does not have an adequate level of protection.[154] The modernised Council of Europe Convention 108 contains specific rules about the transborder transfers of data establishing the rules that members that are parties to the Convention shall not, "for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention"[155]. Exceptions to this rule may be justified if there is a real and serious risk that the further transfer would lead to circumventing the provisions of the Convention. With regard to transborder transfers to data to recipients established outside the countries that are party to Convention 108+, then the transfer is only allowed when an appropriate level of protection of personal data is ensured.[156] Such appropriate level of protection can be secured (a) by the law of that State or international organisation, including the applicable international treaties or agreements, or (b) by ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.[157] Transfer of data to a third country that does not ensure an adequate level of protection can also take place under one of the following circumstances:

a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or

b. the specific interests of the data subject require it in the particular case; or

c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or

d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.[158]

Similar rules exist in the GDPR on the transfers of personal data to third countries.[159] The CJEU has published a number of judgments that relate to the transborder transfers of personal data that can be relevant for the exchanges of data for tax purposes and in the AML/CFT context. In Schrems I the CJEU invalidated the Safe Harbour Privacy Principles

---

[153] Council of Europe, 'Opinion on the implications for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes' (4 June 2014) p. 4 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806945a0> accessed 25 May 2021.

[154] Caroline Porasso, Benjamin Aouizerat, 'Report on the implications for data protection of the growing use of mechanisms for automatic inter-state exchanges of personal data for administrative and tax purposes, as well as in connection with money laundering, financing of terrorism and corruption' (30 January 2014) < https://rm.coe.int/bureau-of-the-consultative-committee-of-the-convention-for-the-protect/168073dc57> accessed 25 May 2021.

[155] Council of Europe, *Modernised Convention for the protection of individuals with regard to the processing of personal data* ETS No.108, Art 14.

[156] Ibid, Art. 14(2).

[157] Ibid, Art. 14(3).

[158] Ibid, Art. 14(4).

[159] Mainly GDPR Articles 45, 46 and 49.

(Decision 2000/520) [160]. In this judgment, the CJEU established a number of safeguards that shall be respected when transfers of personal data take place to a country that does not ensure an adequate level of protection for personal data. The CJEU considered it essential that persons whose personal data have been or could be transferred to a third country have the possibility to lodge a claim with the national data protection authorities[161], when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[162] Access to the transferred data shall be allowed when it is strictly necessary and proportionate to the protection of national security.[163] On this point, the CJEU clarified that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[164] Furthermore, the data subject shall have a right to redress, enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.[165] The CJEU argued that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.[166]

Following Schrems I, a new agreement was adopted for the transfers of data from the EU to the US, the Privacy Shield.[167] However, the CJEU invalidated this agreement, as well. The Court's invalidation of the Privacy Shield was based on the following grounds. First, the primacy of US law enforcement requirements over those of the Privacy Shield[168], second the lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in light of proportionality requirements[169], third, the lack of an effective remedy in the US by EU data subjects[170] and fourth deficiencies in the Privacy Shield Ombudsman mechanism[171].[172]

The Schrems I and Schrems II judgments establish safeguards that should be respected by European Union Member States when personal data are transferred to a third county and should be taken into account when inter-state exchanges of data take place for tax purposes but also for AML/CFT. In particular, the safeguards established by the CJEU raise questions as to the compatibility of inter-state exchanges of data without adequate safeguards. Therefore, it is recommended that States shall make sure that the exchanges of data for tax and AML/CFT purposes are complemented with additional safeguards, in line with the CJEU case law.

---

[160] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.
[161] Ibid, para. 53.
[162] Ibid, para. 66.
[163] Ibid, para. 90.
[164] Ibid, para. 94.
[165] Ibid, para. 90.
[166] Ibid, para. 95.
[167] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN> accessed 25 May 2021.
[168] Case C-311/18 *Data Protection Commissioner v Facebook Ireland, Maximillian Schrems* [2020] ECLI:EU:C:2020:559, para. 164
[169] Ibid, paras. 168-185.
[170] Ibid, paras. 191-192.
[171] Ibid, paras. 193-197.
[172] Christopher Kuner, The Schrems II judgment of the Court of Justice and the future of data transfer regulation, 17 July 2020 < https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> accessed 26 May 2021.

Following the CJEU judgment on Schrems II, the EDPB issued recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[173] and recommendations 2/2020 on the European essential guarantees for surveillance measures.[174] Taken together these two documents outline an assessment process for the sufficiency of foreign protections under European law when personal data is sent abroad and a set of EU-approved safeguards that companies can implement even when foreign protections are judged lacking compared to the European legal standards. According to the EDPB, the "European Essential Guarantees, which need to be respected to make sure interferences with the rights to privacy and the protection of personal data, through surveillance measures, when transferring personal data, do not go beyond what is necessary and proportionate in a democratic society"[175]. These European Essential Guarantees are summarised as follows:

A - Processing should be based on clear, precise and accessible rules

B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

C - Independent oversight mechanism

D - Effective remedies need to be available to the individual[176]

The EDPB recognised that the ultimate decision in whether human rights interferences are justified belongs to the CJEU. However, the EDPB recognised that "in absence of such a judgment and in application of the standing jurisprudence, data protection authorities are required to assess individual cases, either ex officio or following a complaint, and to either refer the case to a national Court if they suspect that the transfer does not comply with Article 45 [GDPR] where there is an adequacy decision, or to suspend or prohibit the transfer if they find Article 46 GDPR cannot be complied with and the protection of the data transferred required by EU law cannot be ensured by other means."[177] In this way the EDPB recognises the power of data protection authorities to refer individual cases to national courts. However, data protection authorities have not referred potential cases to their national courts yet.[178] Recommendations 2/2020 presented a roadmap consisting of six steps in order to apply the principle of accountability to data transfers in practice. It outlined supplementary technical, contractual and organisational measures to be taken, when the tool used for the transfer of data are not sufficient.

Following these developments, on 13 April 2021, the European Data Protection Board invited Member States "to assess and, where necessary, review their international agreements that involve international transfers of personal data, such as those relating to taxation (e.g. to the automatic exchange of personal data for tax purposes), social security, mutual legal assistance, police cooperation, etc. which were concluded prior to 24 May 2016 (for the agreements relevant to the GDPR) or 6 May 2016 (for the agreements relevant to the LED). This review should be done in order to determine whether, while pursuing the important

---

[173] EDPB, Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (10 November 2020) <https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf > accessed 25 May 2021.

[174] EDPB, Recommendations 2/2020 on the European Essential Guarantees for surveillance measures (10 November 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf> accessed 25 May 2021.

[175] Ibid.

[176] Ibid, pp.8-15.

[177] Ibid, para. 6

[178] See for instance the UK ICO that did not examine the compatibility of FATCA with the ECHR and the CFR nor did it refer the case to a national court: Information Commissioner's Office, Freedom of Information Act 2000 (FOIA) Decision notice, 1 March 2019, Ref: FS50751683, para. 33, para. 38-47.

public interests covered by the agreements, further alignment with current Union legislation and case law on data protection, as well as EDPB guidance might be needed.[179] Such review can be very relevant in the field of inter-state exchange of personal data in the fields of taxation and AML/CTF; it enables for instance European data protection authorities to refer individual cases to national courts in order to examine the compatibility of foreign systems with the European safeguards, such as FATCA for which concerns have already been raised, as regards its compliance with European data protection standards. The accessing of data by the US authorities, which was a major concern in both Schrems I and Schrems II, is affecting any exchange of data, including the ones falling under FATCA (more analysis on FATCA in section 10.2.

Although the judgments of the CJEU are not binding for countries outside the European Union ones, they provide with a comprehensive list of safeguards that could serve as best practices also outside the EU.

10.1 Exchange of data for AML/CFT

In the context of AML/CFT information is transferred to countries that do not ensure an adequate level of data protection in various instances. Most prominent is the exchange of data from an FIU to a foreign counterpart established in a country not having an adequate level of protection. When FIUs are members of the Egmont Group, they follow the Egmont principles for information exchange between financial intelligence units[180].

FATF Recommendation 18 invites financial institutions' group level AML/CFT functions and branches to share STRs between themselves.[181] When the branches or subsidiaries are established in a third country, the relevant data protection requirements shall be applied. 4AMLD, taking into account a possibility that a branch of a subsidiary of a credit or financial institution can be located in a third country, where the AML/CFT requirements are less strict than those of the Member State, and in order to avoid the application of very different standards within the institution or group of institutions, established the rule that the obliged entities must apply the Union standards or notify the competent authorities of the home Member State if the application of such standards is not possible.[182]

Article 53 4AMLD compels European Union Member States to ensure the free exchange of information between European FIUs.[183] Article 53(3) allows the refusal to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles in its national law.

Great interest presents the transfer of data from an FIU to other foreign authorities (not FIUs), when this is allows by national legislation, such as for instance under Spanish law, which allows the direct exchange of data contained in declarations of means of payment and related to the seizure of means of payment from the Spanish FIU to foreign competent authorities (primarily customs ones)"[184]

---

[179] EDPB, Statement 04/2021 on international agreements including transfers (13 April 2021) <https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf> accessed 25 May 2021.

[180] Egmont Group of Financial Intelligence Units, 'Principles for information exchange between financial intelligence units' (July 2013) <https://egmontgroup.org/en/filedepot_download/1658/79> accessed 25 May 2021.

[181] Benjamin Vogel, Jean-Baptiste Maillart, *National and international anti-money laundering law* (1st edn Insertia 2020) p. 858

[182] Directive 2015/849 (4AMLD), Recital 48 and Art. 45(5)

[183] See also Recital 58 4AMLD.

[184] art. 37 Spanish AML Law (law n. 10/2010).

10.2 Exchange of data for tax purposes

States shall ensure that when exchanges take place towards a third country that does not ensure an adequate level of protection, the safeguards established in the data protection legislation shall be respected. All CRS agreements entered into by state parties of Convention 108+ with third countries shall respect the data protection safeguards established in the Convention.

The interstate exchanges of data for tax purposes and especially with regard to FATCA have been in the centre of the attention of the Article 29 Data Protection Working Party (WP29), the predecessor of the European Data Protection Board. The WP29 addressed in 2012 two letters Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA).[185] Already in their letter of June 2012 the WP29 pointed out that "FATCA must be mutually recognised as necessary from an EU perspective. This requires ensuring that there is a lawful basis for the processing through careful assessment of how FATCA's goals balance with that of the EU's fundamental right enshrined in Article 8 of the Charter of Fundamental Rights – the right to a private and family life, i.e. by demonstrating necessity by proving that the required data are the minimum necessary in relation to the purpose. A bulk transfer and the screening of all these data is not the best way to achieve such a goal. Therefore, more selective, less broad measures should be considered in order to respect the privacy of law-abiding citizens, particularly; an examination of alternative, less privacy-intrusive means must to be carried out to demonstrate FATCA's necessity.[186] Already in 2012, the WP29 highlighted that "in the absence of a lawful basis to legitimize the processing required, WP29 does not see how compliance of FATCA and the Directive could be simultaneously achieved"[187]. The WP29 found that at that time (2012) there is no legal basis within EU or national law of a Member State to ensure lawful processing of the data within the scope of FATCA. If this remains the case on the entry into force of FATCA, EU/EEA data protection authorities (DPAs) may consider prohibiting the data processing in question"[188].

In 2015 the WP29 issued a statement on automatic inter-state exchanges of personal data for tax purposes[189] and in 2016 it published guidelines for Member States on the criteria to

---

[185] Letter from the Article 29 Data Protection Working Party to Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA), 21.06.2012, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf> accessed 26 May 2021; Letter from the Article 29 Data Protection Working Party to Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA), 01.10.2012, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20121001_letter_to_taxud_fatca_en.pdf> accessed 26 May 2021.

[186] Letter from the Article 29 Data Protection Working Party to Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA), 21.06.2012, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf> accessed 26 May 2021. Para. 8.3.

[187] Letter from the Article 29 Data Protection Working Party to Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA), 21.06.2012, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf> accessed 26 May 2021. Para. 8.4.

[188] Letter from the Article 29 Data Protection Working Party to Mr. Zourek, then Director General of Taxation and Customs Union regarding Foreign Account Tax Compliance Act (FATCA), 21.06.2012, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf> accessed 26 May 2021. Para. 1.5.

[189] Article 29 Data Protection Working Party, Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, WP230, 04 February 2015 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf> accessed 26 May 2021

ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes[190].

In the same year, the WP29 sent a letter to the collective of European "accidental Americans" on data protection issues arising in relation to FATCA informing them that, although the WP29 cannot form an opinion on the potential exclusion of accidental Americans from the scope of FATCA, they csn file a complaint with their national DPA or national court.[191] The European Parliament dealt in the same year with the adverse effects of FATCA on EU citizens and in particular 'accidental Americans', meaning persons "who, by accident of birth, inherited US citizenship, but who maintain no ties to the US, having never lived, worked or studied in the US and who do not hold US social security numbers".[192] The European Parliament has stressed "the importance of providing an adequate level of protection for personal data transferred to the US under FATCA, in full compliance with national and EU data protection law; [called] on the Member States to review their [implementing intergovernmental agreements-] IGAs and to amend them, if necessary, in order to align them with the rights and principles of the GDPR; [urged] the Commission and the European Data Protection Board to investigate without delay any infringement of EU data protection rules by Member States whose legislation authorises the transfer of personal data to the US [Internal Revenue Service-] IRS for the purposes of FATCA, and to initiate infringement procedures against Member States that fail to adequately enforce EU data protection rules".[193] The European Parliament in its recent resolution on Schrems II expressed its concern about the inefficient level of enforcement of the GDPR, particularly in the area of international transfers.[194] It requested the European Commission to analyse the impact of the Schrems I and II judgments on data exchanges with the United States[195], and in particular FATCA and the intergovernmental agreements implementing FATCA. In its 2018 resolution, the European Parliament stressed "the importance of providing an adequate level of protection for personal data transferred to the US under FATCA, in full compliance with national and EU data protection law; calls on the Member States to review their IGAs and to amend them, if necessary, in order to align them with the rights and principles of the GDPR; urges the Commission and the European Data Protection Board to investigate without delay any infringement of EU data protection rules by Member States whose legislation authorises the transfer of personal data to the US IRS for the purposes of FATCA, and to initiate infringement procedures against Member States that fail to adequately enforce EU data protection rules"[196]. The European Parliament further advised the following actions:

---

[190] Article 29 data Protection Working Party, Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes, WP234, 16 December 2015 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp234_en.pdf> accessed 26 May 2021.

[191] Letter from the Article 29 Data Protection Working Party to the , 21.06.2012,

[192] European Parliament, Parliament resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans' (2018/2646(RSP), OJ C 118/141 (8 April 2020) point D <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC> accessed 25 May 2021

[193] Ibid, para 5.

[194] European Parliament, Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) para. 5 <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf.> accessed 25 May 2021.

[195] Ibid, para. 24.

[196] European Parliament, Parliament resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans' (2018/2646(RSP), OJ C 118/141 (8 April 2020) para. 5 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC> accessed 25 May 2021

"6. Calls on the Commission to conduct a full assessment of the impact of FATCA and the US extraterritorial practice of CBT on EU citizens, EU financial institutions and EU economies, taking into account ongoing efforts in France and other Member States, and to explain if a serious discrepancy exists between EU citizens and/or residents in different Member States, especially as regards EU data protection rules and fundamental rights standards as a result of FATCA and 'US indicia'; calls on the Commission to conduct a comprehensive assessment of the status of FATCA reciprocity, or the lack thereof, across the EU, and compliance by the US with its obligations under the various IGAs signed with Member States;

7. Calls on the Commission to assess and, if necessary, take action to ensure that the EU fundamental rights and values enshrined in the Charter of Fundamental Rights and the European Convention on Human Rights, such as the right to privacy and the principle of non-discrimination, as well as EU data protection rules, are respected in the context of FATCA and the automatic exchange of tax information with the US;

8. Regrets the inherent lack of reciprocity of IGAs signed by Member States, especially in terms of the scope of information to be exchanged, which is broader for Member States than it is for the US; calls on all Member States to collectively suspend the application of their IGAs (or the sharing of all information other than that in respect of accounts held in the EU by US citizens resident in the US) until such time as the US agrees to a multilateral approach to the automatic exchange of information (AEOI), by either repealing FATCA and joining the CRS or renegotiating FATCA on an EU-wide basis and with identical reciprocal sharing obligations on both sides of the Atlantic;

9. Calls on the Commission and the Council to present a joint EU approach to FATCA in order to adequately protect the rights of European citizens (in particular 'accidental Americans') and improve equal reciprocity in the automatic exchange of information by the US;

10. Calls on the Council to mandate the Commission to open negotiations with the US on an EU-US FATCA agreement, with a view to ensuring the full reciprocal exchange of information, upholding the fundamental principles of EU law, as well as the Payment Accounts Directive, and allowing EU 'accidental Americans' to relinquish their unwanted US citizenship on a no-fees, no-filings, no-penalties basis"[197]

The EDPB issued a few months later a Statement on FATCA, announcing that it had already started the preparation of guidelines on transfer tools based on Art, 46 GDPR (appropriate safeguards).[198] The relevant recommendations were published in November 2020.[199]

All entities whose data processing is subject to the jurisdiction of a party to Convention 108+ party that transfer data to third countries, and the US in particular, shall ensure respect to the data protection framework established in CoE Convention 108+. Similarly, Parties to the

---

[197] European Parliament, Parliament resolution of 5 July 2018 on the adverse effects of the US Foreign Account Tax Compliance Act (FATCA) on EU citizens and in particular 'accidental Americans' (2018/2646(RSP), OJ C 118/141 (8 April 2020) paras. 6-10 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC> accessed 25 May 2021

[198] European Data Protection Board, EDPB Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA), 25 Feburary 2019 < https://edpb.europa.eu/our-work-tools/our-documents/statements/edpb-statement-012019-us-foreign-account-tax-compliance-act_sv> accessed 26 May 2021.

[199] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020 < https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf> accessed 26 May 2021.

Convention shall review the compatibility of agreements that facilitate the exchange of data for tax purposes to third countries with the data protection framework of CoE Convention 108+. National supervisory authorities shall assist the signatory parties in ensuring compliance with CoE Convention 108+.

11. Conclusions and recommendations

The AML/CFT framework as well as rules for combating tax fraud/tax evasion shall be applied along with the provisions of the data protection framework. This report outlined the most important principles, as well as rights and obligations that shall be respected in this context. Particular attention shall be paid to the following issues, as discussed in the report:

An important point to be clarified in both the AML/CFT and the taxation field relates to the allocation of data protection roles the entities involved. Especially when PPPs are established, which is more relevant for AML/CFT, a clear allocation of the roles to the entities that participate in the PPP and a delineation of the rights and obligations in relation to the processing of personal data shall be made, ideally already in the law, or other sources or jurisprudence, establishing the PPP. As regards the field of taxation, parties to the Convention shall make sure to include a clear allocation of data protection roles, that bring along concrete rights and obligations, when establishing rules that involve the exchange of data.

It is crucial for all exchanges of data by private entities, which usually takes place for AML/CFT purposes, shall take place on a clear legal basis.

The processing of personal data relating to criminal proceedings and convictions shall be allowed for AML/CFT purposes only when appropriate safeguards are established in law. For instance, obliged entities should only be allowed to process criminal proceedings and convictions related to money laundering and terrorist financing handed down in countries where the rule of law, and especially the presumption of innocence, the right of defence and right of a fair trial are respected.

CoE Convention 108+ establishes a number of rights for the data subjects. The recent case law of the CJEU has strengthened the protection of data subject rights, as protected in the European Data protection framework. Following the reasoning of the CJEU, it shall be accepted that private entities involved in the exchanges of personal data either for tax purposes or -even maybe more prominently- for AML/CFT remain under the scope of the European data protection framework (in particular, the GDPR), even when the exchange has been requested by a competent authority (which could also be an FIU in case of AML/CFT). As such, careful examination of the regime under which the exchange of data is realised, especially when private entities are involved, is essential, before restricting any rights of the data subjects. Special attention shall be given to the right of the affected persons to be informed about the processing of their personal data. Although the right of data subjects to be notified when their personal data are processed can be restricted in the framework of combating ML/FT and tax fraud/tax evasion, this shall not be done in a blanket way. Based on the case law of the CJEU and the ECtHR, the relevant authorities may refrain from informing the data subjects about their processing of their personal data. However, these authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations. Supervisory authorities shall have the power to examine whether the notification of the data subjects is actually realised. The CJEU in *La Quadrature du Net* established some new rules on the notification of the persons involved when automated analysis takes place. This judgment is of great importance when automated analysis of data takes place in both the tax fraud/tax evasion context and in the AML/CFT framework. It is unclear whether the CJEU aimed at imposing such an obligation to notify individually the persons concerned when these persons have been singled out based on automated analysis only to national authorities or whether

such an obligation should be expanded to private entities as well. This latter concern would have great impact on obliged entities in the AML/CFT framework, which are already making use of AI in order to carry out data mining and profiling operations.

Article 5 of COE Convention 108+ stipulates a number of principles for the legitimacy of data processing and the quality of data, which shall be respected whenever personal data are exchanged. The principles established in Article 5(4), i.e. fairness and transparency, purpose limitation, data minimisation, data accuracy and storage limitation, can be restricted in line with Article 11 CoE Convention 108+. Interstate exchanges of personal data shall always take place respecting these principles, while restrictions in line with Article 11 CoE Convention 108+ shall be clearly justified.

The proportionality principle requires careful use of AI in the fields of AML/CFT and taxation to make sure that the processing abides by the data protection framework. The principle of data accuracy is difficult to be complied with especially when data are collected from external sources known as "watchlists", which are provided by third parties. Therefore there is a need for further clarification of the responsibilities between obliged entities and the watchlists providers regarding data protection obligations, "to provide guarantees especially regarding the compilation of sensitive data, as well as to regulate the consultation of those lists by obliged entities and specify how data subject rights are respected in this context"[200], in line with corresponding recommendations of the EDPB at a European Union level.

Given the multilateral nature of mechanisms for inter-state exchanges of personal data for tax and AML/CFT purposes, the question of adequate protection arises in all cases where the exchange of personal data involves a country that does not have an adequate level of protection. The CJEU has published a number of judgments that relate to the transborder transfers of personal data that can be relevant for the exchanges of data for tax purposes and in the AML/CFT context. The Schrems I and Schrems II judgments establish safeguards that should be respected by European Member States when personal data are transferred to a third county and should be taken into account when inter-state exchanges of data take place for tax purposes but also for AML/CFT. In particular, the safeguards established by the CJEU raise questions as to the compatibility of inter-state exchanges of data without adequate safeguards. The accessing of data by the US authorities, which was a major concern in both Schrems I and Schrems II, is affecting any exchange of data, including the ones falling under FATCA. Therefore, it is recommended that European Union States shall make sure that the exchanges of data for tax and AML/CFT purposes are complemented with additional safeguards, in line with the CJEU case law.

All entities, whose data processing is subject to the jurisdiction of a Party member to Convention 108+, that transfer data to third countries, and the US in particular, shall ensure respect to the data protection framework established in CoE Convention 108+. Parties to the Convention shall review the compatibility of agreements that facilitate the exchange of data for tax purposes to third countries with the data protection framework of CoE Convention 108+. National supervisory authorities shall assist the signatory parties in ensuring compliance with CoE Convention 108+. In addition, parties to the Convention shall enable their data protection authorities to refer individual cases to national courts in order to examine the compatibility of foreign systems with the safeguards provided for in Convention 108+, such as FATCA for which concerns have already been raised, as regards its compliance with European data protection standards.

This report focused only on data protection issues arising in relation to the inter-state exchanges of data for tax purposes and to counter money laundering and the financing of terrorism. A lot of interesting data protection issues arise in relation to the pooling of data and

---

[200] European Data Protection Board, Letter to the European Commissioner for Financial services, financial stability and Capital Markets Union and to the European Commissioner for Justice (19.05.2021) < https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf> accessed 30 June 2021.

their accessing by private entities. To this direction, the FATF has prepared a stocktake on data pooling and analysis, aimed at helping private sector making better use of artificial intelligence and big data analytics for AML/CFT, and increasing the efficiency of regulatory compliance, while ensuring a high level of data protection.