The proposed anti-money laundering authority and the future of FIU collaboration in Europe

8

The Proposed Anti-Money Laundering Authority and the Future of FIU Collaboration in Europe

ELENI KOSTA*

I. INTRODUCTION

The field of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) is considered a complex field in European Union (EU) legislation.[1] Currently, at the EU level, the most important legal instruments in the framework on AML/CFT are Directive 2015/849 (the 4th Anti-Money Laundering Directive or 4AMLD)[2] and, introducing modifications thereto, Directive 2018/843 (the 5th Anti-Money Laundering Directive or 5AMLD).[3] Further, Directive 2019/1153[4] lays down measures to enhance access to and use of financial information and bank account information by competent law enforcement authorities by providing them with direct access to information contained in national centralised registries. It also facilitates access

* Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, email: e.kosta@tilburguniversity.edu. The research for this chapter was completed in January 2023.

[1] European Commission, 'Anti-Money Laundering and Countering the Financing of Terrorism Legislative Package' (20 July 2021), available at https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en.

[2] 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 (herein referred to as '4AMLD') [2015] OJ L141/73–117.

[3] 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 [2018] OJ L156/43–74.

[4] 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 [2019] OJ L186/122–37.

to law enforcement information for Financial Intelligence Units (FIUs) and stimulates the access of investigative authorities to FIU data.[5]

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.[6] In July 2021, aiming to clarify the existing situation and to enhance the EU's anti-money laundering rules,[7] the European Commission presented a package of legislative proposals, which aims to radically change the landscape of the European AML/CFT framework. The package consists of a proposal for the Anti-Money Laundering Regulation (AML Regulation),[8] a proposal for the 6th AML Directive (6th Anti-Money Laundering Directive or 6AMLD),[9] a proposal for a Regulation on the Anti-Money Laundering Authority (AMLA Regulation)[10] and a proposal for the Regulation on information accompanying transfers of funds and certain crypto-assets.[11] The new AML/CFT legislative package is expected to have an impact on various complex relationships between multiple actors, including the AMLA, obliged entities,[12] global organisations and governmental bodies, such as the FIUs and law enforcement authorities of the Member States.

The European Data Protection Board (EDPB) adopted a Statement on the protection of personal data processed in relation to the prevention of money

[5] ibid Art 1(1).

[6] 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'), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:C(2020)2800&from=EN.

[7] European Commission, 'Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules' (20 July 2021), available at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690.

[8] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing' COM(2021) 420 final (20 July 2021).

[9] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849' COM(2021) 423 final (20 July 2021) ('6AMLD').

[10] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010' COM(2021) 421 final (20 July 2021).

[11] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-Assets' COM(2021) 422 final (20 July 2021).

[12] Obliged entities are specified in Art 3 of the 'Proposal for a Regulation on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing' COM(2021) 420 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420.

laundering and terrorist financing.[13] It also addressed a letter to the European Commission on the review of the European AML/CFT framework.[14] In both documents, 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 [CFR]'.[15] In the statement, the EDPB further underlined the importance of compatibility with the principles of necessity and proportionality and the jurisprudence of the Court of Justice of the European Union.[16]

Thus, the compatibility of the European privacy and data protection rules with the proposed anti-money laundering measures is not an add-on to the proposed anti-money laundering rules. The rights to privacy and data protection are fundamental rights that shall be respected, as safeguarded in the European Charter (CFR) and specified in European secondary legislation.

This chapter focuses on the proposed AMLA. Several aspects of the new landscape have been debated throughout the reform process, one of them being the procedure of data sharing among several entities,[17] which will be affected by the new regime. Data sharing unequivocally brings data protection rules to the forefront. This chapter aims at identifying areas of a potential clash between the rules of the AMLA Regulation and the EU data protection framework, especially in relation to data sharing. To this end, the role of the FIUs is pivotal as the collaboration between these institutions is enhanced in the proposed AML/CFT framework.

This chapter will first briefly outline the main EU data protection legal instruments, aiming at clarifying their scope of application and the extent to which they are relevant in the context of AML/CFT. It will then attempt to disentangle the knot of the data protection rules that apply to FIUs and to outline the implications for the AMLA. The chapter will thereafter discuss the complexities relating to the hosting of the FIU.net by the AMLA and finally, it will study the practice of joint analyses and cross-border data transfers.

[13] European Data Protection Board, 'Statement on the Protection of Personal Data Processed in Relation with the Prevention of Money Laundering and Terrorist Financing (Adopted on 15 December 2020), available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf.

[14] 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 May 2021), available at https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf.

[15] European Data Protection Board Statement (n 13) 2 and European Data Protection Board Letter (n 14) 2.

[16] European Data Protection Board Statement (n 13).

[17] European Commission, 'Communication from the Commission on an Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorist Financing 2020/C 164/06, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0513%2803%29.

II. EU SECONDARY LEGISLATION ON DATA PROTECTION

The protection of personal data in the EU is regulated through an extensive and complicated matrix of secondary legal instruments, mainly directives and regulations, with three of the most prominent pieces of legislation that are relevant for the processing of personal data in the context of AML/CFT, ie Regulation 2016/679 (General Data Protection Regulation, GDPR),[18] Directive 2016/680 (Law Enforcement Directive, LED)[19] and Regulation 2018/1725 (EU Data Protection Regulation, EUDPR).[20]

The GDPR sets high standards and strict obligations for legitimate data processing, while it leaves data processing by competent authorities for law enforcement purposes outside its scope. By virtue of it being a regulation, the GDPR is directly applicable in (European) Member States, without the need for national implementation. Nevertheless, Member States should update their existing national data protection laws in light of the Regulation. In the AML/CFT context, the GDPR is mostly applicable in the processing of personal data by obliged entities, including the sharing of data.

The LED applies when police and criminal justice authorities process the personal data of natural persons (including suspects, accomplices, victims and informants) for law enforcement purposes in a domestic context, but it also applies to cross border processing between Member States' police and judicial authorities, and to international transfers between those authorities. The provisions of the LED have been tailored to the context of law enforcement, affording law enforcement a certain degree of flexibility to enable them to carry out their tasks and duties.[21] The LED is applicable in the context of the AML/CFT framework, when data are requested or shared by law enforcement authorities (LEAs). It is debatable whether the GDPR or the LED are applicable to the processing of personal data and the problem only increases, where FIUs of a distinct nature (eg, law enforcement or hybrid) share data with FIUs that have an administrative character.[22]

[18] European Parliament and Council Regulation 2016/679 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) [2016] OJ L119/1–88.

[19] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (LED) [2016] OJ L119/89.

[20] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) ('EUDPR') [2018] OJ L295/39.

[21] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg, Publications Office of the European Union, 2018) 283.

[22] M Brewczyńska, 'Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework' (2021) *Computer Law & Security Review* 43; T Quintel, 'Follow the Money,

The EUDPR regulates the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies, and introduces rules relating to the free movement of personal data between Union institutions and bodies or to other recipients established in the Union and includes the processing of personal data in the context of police and judicial cooperation for criminal matters. Chapter IX of the EUDPR is dedicated to the processing of operational personal data[23] by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 (Judicial Cooperation in Criminal Matters) or Chapter 5 (Police Cooperation) of Title V (Area of Freedom, Security and Justice) of the Treaty on the Functioning of the European Union (TFEU). It is thus a legal instrument that covers both general data processing and to a certain extent data processing in the context of police and judicial cooperation. As the AMLA is established as a Union body,[24] the EUDPR applies to the processing of personal data by the AMLA.

III. FIUs' ACCESS TO INFORMATION AND DATA SHARING UNDER THE AUSPICES OF THE AMLA

Member States have incorporated the FIUs in different ways and thus the nature of the FIUs has resulted in a patchwork of choices. Twelve European countries have indeed established FIUs that are administrative in nature,[25] nine countries have FIUs with a law enforcement/judicial nature[26] and six countries have hybrid FIUs.[27]

The European Data Protection Supervisor (EDPS) provided a short description of the differences between these FIU types: FIUs of an administrative nature are placed under the authority of Ministries of Finance, Justice, of the Interior, central banks or supervisory authorities, while FIUs that have a law enforcement nature are part of a structure with the competence to fight economic or other serious crimes. Finally, FIUs of a hybrid nature are established within national

If You Can – Possible Solutions for Enhanced FIU Cooperation Under Improved Data Protection Rules' (Europarättslig tidskrift 2019 1, March 2019 s. 35–50), available at https://lawpub.se/en/artikel/1225; F Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive' (2020) 11(3) *New Journal of European Criminal Law*, available at https://ieeexplore.ieee.org/document/6691683.

[23] 'Operational personal data' means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies (EUDPR (n 20) Art 3(2)).

[24] AMLA Regulation Proposal (n 10) Art 3.

[25] Belgium, Bulgaria, Croatia, Czechia, France, Italy, Latvia, Malta, Poland, Romania, Slovenia, Spain: EU FIUs' Platform, 'Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information' (15 December 2016).

[26] Austria, Estonia, Finland, Luxembourg, Ireland, Lithuania, Portugal, Slovakia, Sweden: ibid.

[27] Cyprus, Denmark, Greece, Hungary, Netherlands, Germany: ibid.

police offices or in the offices of the attorney general/prosecutor but separate from operational/judicial units and they are composed of both police officers and analysts from non-police organisations.[28] The discussion on the nature of the FIU as administrative, law enforcement/judicial or hybrid is not part of a theoretical debate as it has an impact on the applicable data protection framework on the processing of personal data by FIUs, on the type of information an FIU can get access to for the purposes of analysis and its other powers and the actual facilitation of such access.[29]

In order to clarify whether the GDPR or the LED apply when FIUs process personal data, it is first crucial to clarify the notion of competent authorities as defined in the LED.[30] As regards a competent authority in a strict sense, the LED requires it to be a 'public' body, as opposed to organisations of a private character. The second type of 'competent authority' is the authority 'entrusted' with the law enforcement task. Unlike a competent authority in a strict sense, this type of authority does not have to be public. Conversely, the definition does not preclude that a competent authority can also be a private entity if it is assigned the competence to exercise public authority and public powers for the law enforcement purposes by Member State law. Such a broad margin of manoeuvre makes it, on the one hand, easier to adjust to domestic realities, but, on the other, opens possibilities for diverging approaches and increasing differences across the EU. Thus, it is difficult to pin down which entities will in fact fall under the definition of a 'competent authority' without carrying out a detailed analysis of the national arrangements of the Member States. In addition, Mouzakiti conducted interviews with European FIUs and came to the conclusion that even FIUs that qualify as administrative ones might not necessarily fall under the GDPR's scope, and vice versa.[31]

The EDPS has repeatedly purported that FIUs are intelligence-gathering entities that act prior to any criminal investigation.[32] According to the EDPS, even if FIUs are structurally integrated within law enforcement or the judiciary, they should remain subject to the GDPR in their activities and should not be considered as competent authorities under the LED. This position can be called into question. The European Commission, in its report on the assessment on the framework for the cooperation between FIUs, recognised the lack of clarity regarding the applicable data protection framework as a known problem.

[28] EDPS Decision of 19 December 2019 relating to the technical administration of FIU.net by Europol, para 3.16.

[29] Europol letter to the Chair of the FIU.net Advisory Group, Consultation regarding the embedment of FIU.net into SIENA, 11 September 2019; EDPS Decision, ibid.

[30] LED (n 19) Art 3(7).

[31] Mouzakiti (n 22).

[32] EDPS, 'Opinion 6/2015 A Further Step towards Comprehensive EU Data Protection. EDPS Recommendations on the Directive for Data Protection in the Police and Justice Sectors' (2015) 5–6, available at https://edps.europa.eu/sites/edp/files/publication/15-10-28_directive_recommendations_en.pdf; EDPS, 'Opinion 12/2021 on the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Package of Legislative Proposals (22 September 2021), available at https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf.

In particular, in relation to the exchange of data from FIUs to third countries, the report outlines the following:

> When Member States' FIUs exchange information with third countries, they have to comply with the relevant requirements of the applicable EU data protection regime, which in the case of FIU cooperation are determined by the General Data Protection Regulation. Despite this clear obligation, most FIUs apply the Police Data Protection Directive (Directive (EU) 2016/680) [referred to as the LED, in this report] instead or both the General Data Protection Regulation and the Police Data Protection Directive. While this issue applies to all the aspects of the work of FIUs, it is particularly relevant in relation to cooperation with the third countries, where the requirements and conditions for the exchanges are different under the Police Data Protection Directive.[33]

Based on the above, when FIUs of a law enforcement nature process personal data for law enforcement purposes, for example, when they exchange information for an AML investigation, (then) the processing can be governed by the LED. This assumes that FIUs are considered as competent authorities under the LED in the national legislation of these Member States, and hence one should look into the national laws to identify whether the FIUs are entrusted with the task of preventing crimes or not. While FIUs of a law enforcement nature would have the power to freeze transactions and to seize assets, administrative FIUs would not have similar powers.[34] Consequently, administrative FIUs would not have the competence to process data relating to seized accounts, which would become problematic in cases of exchange of information between FIUs. Further, due to their different natures, FIUs do not have access to the same type of information, nor are they able to share information with other FIUs, even if there is a legal obligation to do so.[35]

The new European legislative package on AML/CFT introduces rules that add further complexity to this issue. Article 18 6AMLD, and in particular paragraph(1)(c), envisages to give FIUs access to information which is held by competent authorities in the context of preventing, detecting, investigating or prosecuting criminal offences. FIUs in many Member States, where they are established with an administrative nature, will lack the legal basis for processing data relating to the prevention, detection, investigation or prosecution of criminal offences. In addition, the fact that FIUs can be provided access to law enforcement information will most likely not stand the scrutiny of the necessity and proportionality principles and the purpose limitation principle.

It is not clear whether FIUs sharing data under the auspices of the AMLA, will only share data regarding suspicious transactions or if they will also share

[33] European Commission, 'Report from the Commission to the European Parliament and the Council Assessing the Framework for Cooperation between Financial Intelligence Units, COM(2019) 371 (24 July 2019), 12 available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52019DC0371.

[34] Quintel (n 22).

[35] Commission Staff Working Document, 'On Improving Cooperation between EU Financial Intelligence Units' SWD(2017) 275 final (Brussels, 26 June 2017).

the data types identified in Article 18 6AMLD, which qualify as law enforcement related data. In the case of the latter, administrative FIUs would obtain access to law enforcement data which may violate the legality, proportionality and purpose limitation principles. Although a solution would be for the legislator to vest the AMLA with the power to limit the access of administrative FIUs to law enforcement related data, this could become a very burdensome task for the AMLA, verifying which FIU may have access to what types of data.

IV. FIU.NET HOSTED BY THE AMLA

The AMLA Regulation further assigns the FIU.net to the AMLA, which 'shall ensure adequate and uninterrupted hosting, management, maintenance, and development of the FIU.net'.[36] The FIU.net is a decentralised computer network supporting EU FIUs in their fight against money-laundering and terrorist financing.[37] FIU.net became operational in 2007 and it was a system aimed at supporting the national authorities of the Member States in their fight against money laundering, by allowing and facilitating the exchange of information between FIUs on cross-border financial transactions.[38] As a 'decentralised' network, it did not have a central database and there was no centralised storage of data in one specific Member State where all the exchanged data were stored.[39] All the connected FIUs had their FIU.net equipment within their own premises and managed their own information. Europol was part of the network as an additional node and the AMLA is expected to play a similar role.

Upon its establishment in 2002, the FIU.net system was handled by the Dutch Ministry of Interior, with financial support from the European Commission.[40] In search for a long-term solution concerning the management of FIU.net, it was decided that FIU.net should be embedded within Europol and a Common Understanding was signed to that effect in 2013.[41] It is important that

> in order to realise the full potential of operational synergies between Europol and FIUs, the network facilitating information exchange between FIUs (FIU.net) will be

[36] AMLA Regulation (n 10) Art 37.

[37] Financial Intelligence Unit – the Netherlands, 'FIU.net', available at www.fiu-nederland.nl/en/about-the-fiu/international-cooperation/fiunet.

[38] Europol, 'Europol Joins Forces with EU FIUs to Fight Terrorist Financing and Money Laundering (28 January 2016), available at www.europol.europa.eu/media-press/newsroom/news/europol-joins-forces-eu-fius-to-fight-terrorist-financing-and-money-laundering.

[39] FIU.net (n 37).

[40] European Parliament, Parliamentary Questions, answer given by Mr Avramopoulos on behalf of the Commission, E015304/2015 (February 2016).

[41] Europol, '2014 Consolidated Annual Activity Report' (The Hague, 18 May 2015), available at www.europol.europa.eu/cms/sites/default/files/documents/consolidated_annual_activity_report_caar_2014_0.pdf.

> replaced by SIENA (Europol's systems) and the services of the FIU.net Bureau will be fully embedded within Europol (including the staff of the FIU.net Bureau) ….[42]

In view of the above, FIU.net was officially integrated into Europol three years later and as of 1 January 2016, FIU.net was embedded within Europol to strengthen Europol's financial intelligence and counter terrorism capabilities. The aim of embedding FIU.net within Europol was to create more synergy between financial and criminal intelligence, ultimately boosting efforts to fighting organised crime and terrorism in the EU.[43] According to official statements, the network was set to support the work of Europol's European Counter Terrorism Centre, while FIUs would be able to request Europol to conduct searches with the Terrorist Finance Tracking Program on their behalf.[44]

The FIU.net application is explicitly referred to in a number of articles in 4AMLD[45] as the exchange mechanism for the EU FIUs. The FIU.net is mainly used for three main purposes: (1) cross-border reporting and dissemination;[46] (2) case building data exchange;[47] (3) 'anonymous' cross-match through Ma^{3}tch.[48] Ma^{3}tch (autonomous, anonymous, analysis) was a matching tool within FIU.net that made it possible for FIUs to match names in order to find potentially useful data that would be possessed by other connected FIUs.[49] Ma^{3}tch enabled each FIU to match data already in its files with data of other European FIUs in order to determine whether any of them might hold information that could be of use for their purpose. Where an FIU realised that that was the case, the other FIUs involved would be alerted and could share the actual personal data.[50] To guarantee anonymity, individual records were minimised and aggregated through technical means to ensure that any distinguishing mark could not be linked to an individual. The only characteristics that were captured in the anonymous filters were subsequently shared with selected parties, to ensure that they were able to find and attract the relevant information.[51]

[42] Europol, 'Work Programme 2013' (The Hague, 11 July 2012) 17, available at www.europol.europa.eu/cms/sites/default/files/documents/wp2013_0.pdf.

[43] Europol, 'Europol Joins Forces with EU FIUs to Fight Terrorist Financing and Money Laundering (28 January 2016), available at www.europol.europa.eu/media-press/newsroom/news/europol-joins-forces-eu-fius-to-fight-terrorist-financing-and-money-laundering.

[44] Council of the EU, 'Enhancing Counter Terrorism Capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and Counter Terrorism Related Information Sharing' Document 14244/15 (23 November 2015).

[45] 4AMLD (n 2) Arts 51, 53 and 56.

[46] ibid Art 53.

[47] ibid Art 51.

[48] ibid Art 56(2); Mouzakiti (n 22).

[49] U Kroon, 'Ma3Tch: Privacy and Knowledge: 'Dynamic Networked Collective Intelligence'' (2013 IEEE International Conference on Big Data), available at https://ieeexplore.ieee.org/document/6691683.

[50] Mouzakiti (n 22).

[51] Kroon (n 49).

When information was sent from one FIU to another, the exchanged data were safely stored on the FIU.net databases that were located on the premises of the FIUs involved in the exchange.[52] All (at that time) 28 EU FIUs were connected to the FIU.net and in order to become a member of the FIU.net, each of those FIUs had to connect their internal database to FIU.net.[53]

In 2019, the EDPS found that the Europol Regulation did not provide a sufficient legal basis for Europol to process personal data for the purpose of performing the role of technical administrator of FIU.net. The EDPS banned all processing by Europol of data related to individuals who are not classed as 'suspects' under the applicable national criminal procedure law in the context of the technical administration of FIU.net.[54] However, considering the huge importance of FIU.net in the fight against money laundering at the Union level, the EDPS suspended the ban until 19 December 2020, in order to allow time for a smooth transition of the technical administration of FIU.net to another entity.[55] The AMLA is foreseen to take up this role as host of FIU.net.

In its Communication 'Towards Better Implementation of the EU/s Anti-Money Laundering and Countering the Financing of Terrorism Framework',[56] the Commission pointed out that there are, still today, several recurrent technical matters in the proper functioning of the FIU.net system, which have made it more cumbersome for FIUs to share information and thus, have resulted in less exchange of information and data matching between them.[57] Moreover, the Communication points at the lack of regulation on the exchange of information between Member States' FIUs and FIUs of third countries which has led to a non-harmonised approach to such exchanges, while it also indicates that the transformation of the AML/CFT Directive into a Regulation might be regarded as a potential solution towards a unified, harmonised and directly applicable Union regulatory anti-money laundering framework.[58] Apart from that, according to the EDPS, legal and practical obstacles, such as the ones mentioned above, inevitably have an impact on the accuracy and preciseness of information maintained within the FIU.net system and thus pose a risk for the protection of privacy and personal data.[59]

[52] FIU.net (n 37).

[53] ibid.

[54] European Data Protection Supervisor Decision of 19 December 2019 relating to the technical administration of FIU.net by Europol, para 5.3.

[55] ibid para 5.6.

[56] European Commission, Communication from the Commission to the European Parliament and the Council, 'Towards Better Implementation of the EU's Anti-Money Laundering and Countering the Financing of Terrorism Framework' COM/2019/360 final (24 July 2019), available at https://ec.europa.eu/info/publications/190724-anti-money-laundering-terrorism-financing-communication_en.

[57] ibid.

[58] ibid.

[59] European Data Protection Supervisor, Opinion 5/2020 on the European Commission's Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorism Financing (2020) <https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf.

Even if Europol does not continue to host the FIU.net, it is envisioned as an information exchange hub in the Union. Europol receives and holds valuable information from third countries and international organisations on persons suspected of being involved in crimes that fall within Europol's objectives.[60] Recital 19 of the Europol Recast Regulation addresses the issue of the competence of Europol to process data:

> Where Member States use Europol's infrastructure for the exchange of personal data on crimes that do not fall within Europol's objectives, Europol should not have access to those data and should be considered to be a processor pursuant to Article 87 of Regulation (EU) 2018/1725. In those cases, Europol should be able to process data that do not relate to the categories of data subjects listed in Annex II. Where Member States use Europol's infrastructure for the exchange of personal data on crimes that fall within Europol's objectives and where they grant Europol access to those data, the requirements linked to the categories of data subjects listed in Annex II should apply to any other processing of those data by Europol.[61]

The Europol Recast Regulation contains concrete rules on the exchange of data with Eurojust or the European Anti-Fraud Office.

It is important to bear in mind that if Europol transfers personal data to Member States, third countries or international organisations, the responsibility for the legality of such a transfer shall remain with Europol. Europol is responsible for all data processing operations carried out by it with the exception of processing that is carried out using Europol's infrastructure between Member States, Union bodies, third countries and international organisations to which Europol has no access. The national entities in the exchange of data shall be responsible for such transfers.[62] Hence, based on Article 38 Europol Recast Regulation, it can be concluded that in the event of a transfer of data from EUROPOL to the AMLA, Europol will ensure the legality of transfer and shall take responsibility for the data processing operations carried out on data being transferred until such transfer is complete.

V. FIUs: JOINT ANALYSES OF SUSPICIOUS TRANSACTIONS AND ACTIVITIES – IMPLICATIONS FOR THE AMLA

The new legislative package on AML/CFT contains rules on the carrying out of joint analyses by FIUs both in 6AMLD[63] and in the AMLA Regulation[64] and

[60] European Parliament and the Council of the European Union, Regulation 2022/991 of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L169/1 (Europol Recast Regulation), Recital 9.

[61] ibid Recital 19.

[62] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), Art 38(7).

[63] 6AMLD (n 9) Art 25.

[64] AMLA Regulation (n 10) Art 33.

it foresees the set-up of a dedicated, secured channel of communication for the performance of these joint analyses.[65]

Recital 54 6AMLD explicates the rationale behind the joint analyses. Since several FIUs have reported issues which pose obstacles to the proper and ideal functioning and cooperation between the FIUs, they should be able

> to conduct joint analyses of suspicious transactions and activities and to set up and participate in joint analysis teams for specific purposes and limited period with the assistance of the AMLA. The participation of third parties may be instrumental for the successful outcome of joint analyses. Therefore, FIUs may invite third parties to take part in the joint analysis where such participation would fall within the respective mandates of those third parties.[66]

The purpose limitation and storage limitation principles are implied in Recital 54 6AMLD. Article 25(2) 6AMLD contains a reference to Article 33 AMLA Regulation, clarifying that the AMLA will assist in the setting up of a joint analysis team, instead of being responsible for coordinating it. In the Explanatory Memorandum of the AMLA Regulation, it is determined that 'The Authority will serve as a support and coordination hub assisting their work on, inter alia, joint analyses of Suspicious Transaction Reports and Suspicious Activity Reports with significant cross-border footprint, and providing stable hosting of the FIU.net platform'.[67] In order to specify whether the AMLA will be the data controller of the processing of personal data in this context, it will be important to see how the joint analyses will be organised in practice, in order to identify whether the AMLA will define the purposes and the means of the processing, as the definition of a data controller requires.

VI. CROSS-BORDER DATA TRANSFERS

One of the tasks of the AMLA is to develop appropriate methods and procedures for the FIUs to be able to conduct analyses regarding cross-border cases jointly.[68] The notion of 'cross-border' cases is not defined; however, Article 2(7) 6AMLD defines the notion of an 'entity operating on a cross-border basis' as 'an obliged entity having at least one establishment in another Member State or in a third country'. Following this definition, cases that take place in one Member State and at least one other Member State or a third country shall be considered cross-border cases. In the context of cross-border data transfers, the AMLA Regulation uses a different wording than the one used in the European data protection framework. My suggestion would be to call intra-EU data exchanges

[65] ibid Art 33(4) and 6AMLD (n 9) Art 23.
[66] 6AMLD (n 9) Recital 54.
[67] AMLA Regulation (n 10) 4.
[68] ibid Art 5(5)(c).

'transmissions' and data exchanges with third countries 'transfers', so that the term coincides with the data protection notion of 'international transfers'.

The AMLA is empowered to enter into administrative agreements with authorities in third countries that have FIU-related competences.[69] In the event of interaction between FIUs and several EU public authorities with relevant authorities of third countries that correspond to the tasks assigned to the AMLA under Article 5(5) AMLA Regulation, the AMLA shall have a leading role in facilitating such interactions.[70]

From a data protection point of view, it is important that Article 84 of the AMLA Regulation explicitly provides that the processing of personal data on the basis of the AMLA Regulation shall be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the AMLA under Article 5 EUDPR and Article 6 GDPR. The AMLA has the power to draft guidelines and recommendations to ensure the consistent application of Union law,[71] while it is required to consult the EDPS when recommendations and guidelines have a significant impact on personal data.[72] Chapter V of the EUDPR has the necessary provisions related to the transfer of data to third countries. In the absence of an adequacy decision, the EUDPR permits the transfer of data based on appropriate safeguards.[73] The transfer based on legally binding and enforceable instrument between public authorities and Union bodies[74] is particularly relevant in the context of the AMLA as the AMLA has the power to facilitate administrative agreements between the relevant authorities in the bodies of third countries and the Union.

According to Article 51 EUDPR, the EDPS, in cooperation with the Commission and the EDPB, shall take the necessary steps to develop international cooperation mechanisms to facilitate the protection of personal data in relation to third countries and international organisations. This could mean that while drafting administrative agreements between the relevant authorities of third countries and the Union bodies, the AMLA will need to ensure close cooperation with the EDPS for the exchange of personal data.

Article 35 6AMLD requires supervisors, such as the AMLA, to assess the feasibility of the implementation of policies according to Union law in third countries. In the absence of the proper implementation of the relevant policies and procedures including those related to professional secrecy and data protection, the supervisors should inform each other and take coordinated actions to pursue a solution. Member States have the power to authorise financial supervisors to conclude cooperation agreements with their counterparts in third

[69] ibid Art 81; ibid Recital 63.
[70] ibid Art 81.
[71] ibid Art 43.
[72] ibid Art 84.
[73] EUDPR (n 20) Art 48.
[74] ibid Art 48(2)(a).

countries with respect to exchanging confidential agreements.[75] These cooperation agreements must comply with the relevant data protection rules.[76] The AMLA is expected to lend assistance to determine equivalence of professional secrecy requirements of third countries for the cooperation agreements.[77]

VII. CONCLUSIONS

The AMLA is a long-awaited authority that aspires to play a central role in an integrated system composed of the AMLA and the national authorities that have a AML/CFT supervisory mandate. In this chapter, however, focus was paid to the support that the AMLA is expected to give to FIUs and the role of the AMLA in establishing and supporting a cooperation mechanism between national FIUs. Despite the lack of a pan-European FIU that could be the single point of contact for foreign FIUs, the AMLA has not been vested with such a role. This would require a different legislative and political approach towards the role of the AMLA and the structure of the European AML/CFT system.

This chapter has taken a critical look at the provisions of the AMLA from a data protection point of view. Often, AML/CFT activities have required an exchange of personal information about individuals, possibly including suspects, and the enforcement of the data protection rules has been rather lax. The newly proposed legal framework vouches to take data protection seriously and the AMLA Regulation is offered with an opportunity to take data protection rules into account in its activities from the outset. This chapter has raised a few areas of concern where the rules of the AMLA could be in conflict with the data protection rules. Most prominent in the analysis is the relationship between the AMLA and the national FIUs. The AMLA is tasked with enhancing and facilitating cooperation between FIUs, and with hosting FIU.net. In this context, the AMLA should pay close attention to the applicable data protection rules and the implications these may have both for national FIUs as well as for the joint analyses they will be carrying out. The establishment of the AMLA is a good opportunity for the AML/CFT system and its activities shall pave the way to ensure that data protection rules are not a hurdle that needs to be overcome, but are instead an essential component that ensure AML/CFT activities that are fundamentally rights-compliant.

[75] 6AMLD (n 9) Art 37.
[76] ibid.
[77] ibid.