Data protection rules applicable to Financial Intelligence Units: still no clarity in sight

Teresa Quintel¹

Accepted: 16 December 2021 / Published online: 11 January 2022
© The Author(s) 2022

Abstract

Financial information can play a key role in tackling money laundering, terrorist financing and combatting serious crime more generally. Preventing and fighting money laundering and the financing of terrorism were top priorities of the European Union's (EU) Security Strategy for 2020–2025, which might explain the fast developments regarding legislative measures to further regulate anti-money laundering (AML) and counter terrorism financing (CTF). In May 2020, the European Commission put forward an Action Plan to establish a Union policy on combatting money laundering and shortly afterwards, proposed a new AML Package.

Financial Intelligence Units (FIUs) play a crucial role in analysing and exchanging information concerning unusual and suspicious transactions, serving as intermediaries between the private sector and law enforcement authorities (LEAs). Such information includes personal data, which is protected under the EU data protection *acquis*. The latter is constituted of two main laws, the General Data Protection Regulation (GDPR), which applies to general processing and the so-called Law Enforcement Directive (LED) that is applicable when competent law enforcement authorities process personal data for law enforcement purposes.

This Article argues that the current legal framework on AML and CTF legislation is unclear on the data protection regime that applies to the processing of personal data by FIUs and that the proposed AML Package does little or nothing to clarify this dilemma. In order to contribute to the discussion on the applicable data protection framework for FIUs, the assessment puts forward arguments for and against the application of the LED to such processing, taking into account the relevant legal texts on AML and data protection.

✉ T. Quintel
t.quintel@maastrichtuniversity.nl

¹ Senior lecturer, European Centre on Privacy and Cybersecurity, Maastricht University, Maastricht, The Netherlands

Keywords Data protection · Financial intelligence units · Anti-money laundering · Terrorist financing · GDPR · LED

1 Introduction

Terrorist and organized crime networks such as drug cartels or human traffickers operate across borders and rely on financial assets that are transferred from one country to another.¹ The interconnectivity of the financial system and modern technologies allow those criminal groups to shift money between several bank accounts in a matter of hours in order to *launder* that money.² In the European Union (EU), all recent major money laundering cases that were reported had a cross-border dimension.³ Financial information, including personal data, is therefore a crucial tool for the identification of criminal networks and for the prevention, detection, investigation and prosecution of serious crime and terrorism.

Such information can play a key role in tackling money laundering, terrorist financing, and combatting serious crime in more general terms. This is one of the reasons why the fight against money laundering and the financing of terrorism were top priorities in the EU's Security Union Strategy for 2020-2025.⁴ It might also explain the fast developments regarding the regulation of Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) legislation and the European Commission's (Commission) Action Plan to establish a Union policy on combatting money laundering from May 2020,⁵ eventually leading to the proposal of an Anti-Money Laundering Package ('AML Package') on 20 July 2021.⁶

The proposed AML Package is the most recent legislative endeavour by the Commission to reform the AML/CTF framework and in order to react to recent scan-

¹That is the concealment of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses [Oxford dictionary]. Communication from the European Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final, Strasbourg, 2 February 2016, 3. Cf.: European Agenda on Security, COM(2015) 185 final.

²Proposal for a Directive 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, COM(2018) 213 final, Strasbourg, 17 April 2018, 1.

³Proposal 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, Brussels, 20 July 2021, 3.

⁴Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy COM(2020) 605 final, Brussels, 24 July 2020.

⁵Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing [2020] OJ C 164/21.

⁶European Commission, 'Anti-money laundering and countering the financing of terrorism legislative package', https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en. For a first analysis, see: Sotiris Paphitis, 'The EU's AML Package: an examination', European Law Blog (October 2021); <https://europeanlawblog.eu/2021/10/12/7922/>.

dals around unnoticed illicit transactions.⁷ The package seeks to enhance the effective implementation of the existing EU AML/CFT framework, inter alia, by facilitating timely access to financial data, fostering an enhanced information exchange between the relevant authorities, and by establishing a new EU Authority for supervision. The latter authority is supposed to indirectly monitor obliged entities that operate on national level through the supervision of so-called Financial Intelligence Units (FIUs).

Obliged entities such as banks and other private bodies⁸ are required to compile unusual financial transactions⁹ that are suspected to facilitate money laundering or terrorist financing in suspicious transaction reports (STRs).¹⁰ The abovementioned FIUs play a crucial role in analysing and exchanging information concerning suspicious transactions, serving as intermediaries between the private sector and law enforcement authorities (LEAs).¹¹ Because of the abovementioned international nature of financial crime, cooperation between national FIUs is of paramount importance. Yet, FIUs are not always able to exchange data effectively, which generates information gaps that are often caused by the different organizational structure according to which national FIUs are established. Apart from the structure that may be decisive when determining which information FIUs are able to use for their analyses, their tasks and relationship towards the national LEA may differ, which can lead to divergences in terms of data protection rules that apply to FIUs when processing personal data.¹² Where data protection rules are applied differently, this may lead to incoherencies with regard to transparency obligations for controllers, data subject rights or the restrictions thereof.

Whereas some FIUs apply Regulation (EU) 2016/679¹³ (General Data Protection Regulation, 'GDPR') to their processing activities, others apply Directive (EU) 2016/680¹⁴ (Law Enforcement Directive, 'LED') that applies where competent au-

⁷Richard Milne and Daniel Winter, 'Danske: anatomy of a money laundering scandal: How the Danish bank found itself at the centre of a €200bn money laundering scandal, Financial Times, 19 December 2018; <https://www.ft.com/content/519ad6ae-bcd8-11e8-94b2-17176fbf93f5>.

⁸For instance, auditors, real estate agents, tax advisors, trusts or casinos.

⁹The annual report of the Dutch FIU differentiated between unusual and suspicious transactions, see: Financial Intelligence Unit – the Netherlands, 'annual review FIU – the Netherlands' (2020) 7 ff.; https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5324-fiu_jaaroverzicht_2020-eng-web_v1.pdf.

¹⁰European Parliamentary Research Service (EPRS), 'LE-access to financial data', PE 615.665 (April 2018) 2.

¹¹Herbert V Morais, 'Fighting International Crime and Its Financing: The Importance of Following a Coherent Global Strategy Based on the Rule of Law' (2005) 50 Villanova Law Review 583, 599.

¹²Magdalena Brewczynska, 'Financial Intelligence Units: Reflections on the applicable data protection legal framework', Computer Law & Security Review (2021) 43, 2.

¹³Regulation (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) [2016] OJ L 119/1.

¹⁴Directive (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 [2016] OJ L 119/89.

thorities process personal data for the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security. Because, the LED neither clearly defines what constitutes a competent authority nor what is to be included within 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*, the scope of the Directive is broadened where national legislators decided to apply the LED not only to traditional criminal LEAs, but also to other authorities that may contribute to the prevention, detection or investigation of crime, such as FIUs. The application of the LED may lead to a lower level of data protection standards, as in the law enforcement context, data protection principles are more resilient, data subject rights may be restricted more flexibly and obligations for controllers are not as stringent as under the GDPR.¹⁵

In addition, the line between administrative sanctions and criminal law measures seems to become increasingly blurred, as some of the legislative measures in the area of AML/CTF are no longer based on internal market provisions,¹⁶ but also on police and judicial cooperation legal bases.¹⁷ Although the most recent legislative proposals within the AML Package are exclusively based on the internal market legal basis under Article 114 of the Treaty on the Functioning of the European Union (TFEU), the wording regarding the nature and tasks of national FIUs in those proposals seems ambiguous and could, in certain instances, be interpreted as allowing them to apply the LED.

The following sections of this article will briefly illustrate EU legislation on AML and CT measures that has been introduced in the past years, as well as the recently proposed legislative texts. Section 2 will present the different organizational structures according to which FIUs are set up in the Member States and the tasks that they carry out. Thereafter, Sect. 3 will give a short overview of the different data protection instruments, namely the GDPR and the LED, and provide arguments in favour and against the application of the LED to processing activities carried out by national FIUs. Finally, Sect. 5 will reflect on data retention and access measures to personal

¹⁵Also see: Foivi 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, 351.

¹⁶Under Article 114 of the TFEU, decisions on measures to approximate EU countries' consumer legislation are decided using the ordinary legislative procedure and after consultation of the European Economic and Social Committee.

¹⁷Dealt with in Title V of the Treaty on the Functioning of the European Union (Chapters I, IV and V). The legal texts referred to in this contribution are based on Article 83(1) (Judicial cooperation in criminal matters) and Article 87(2) TFEU (police cooperation and, inter alia, collection, storage, processing, analysis and exchange of relevant information).

data in the area of AML and CTF and compare such measures to those that apply in the area of data retention by telecommunication providers.

2 EU Legislation on Anti Money Laundering and Counter Terrorist Financing

The EU legal regime on AML and CTF has been developed since the 1990s and has progressively strengthened the role of FIUs.¹⁸ The First AML Directive was adopted in 1991¹⁹ to provide the initial stage for setting up a harmonized framework in the EU Single Market, establishing key preventative measures such as customer identification, record-keeping and central methods of reporting suspicious transactions.²⁰ The provisions of that Directive were refined in the Second²¹ and the Third AML Directives,²² which were adopted in 2001 and in 2006 respectively. The Second AML Directive established a broader definition of money laundering and included underlying offences within its scope.²³ Five years later, the Third AML Directive introduced a so-called risk-based-approach,²⁴ which required businesses falling within its scope to carry out a risk-assessment of their customers, based on a variety of factors.²⁵ In accordance to the risk attributed to a particular customer, the obliged entity had to apply Customer Due Diligence measures along the ‘Know Your Customer’ concept.²⁶ All these additional obligations required an increased processing of personal data, also by FIUs.

¹⁸SWD (2017)275, 2.

¹⁹Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering [1991] OJ L166/83.

²⁰‘IBA Anti-Money Laundering Forum – Europe’, accessed January 9, 2019, <https://www.anti-moneylaundering.org/Europe.aspx>.

²¹Directive 2001/97/EC of the European Parliament and of the Council of the European Union of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering Commission Declaration [2001] OJ L344/76.

²²Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis [2006] OJ L 214/34.

²³‘IBA Anti-Money Laundering Forum – Europe’.

²⁴Special Recommendation IX (being covered by Regulation (EC) 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, 2005 O.J. (L 309) 9). See: Maria Bergström, ‘The many uses of Anti-Money Laundering Regulation’, German Law Journal (Volume 19 Number 5) 2018.

²⁵For instance, the Directive specified a number of customer due diligence (CDD) measures that are more extensive and far-reaching for situations of higher risk, such as appropriate procedures to determine whether a person is a politically exposed person (PEP). See: Maria Bergström, ‘The many uses of Anti-Money Laundering Regulation’, German Law Journal (Volume 19 Number 5) 2018, 1160.

²⁶Ibid.

In May 2015, the Fourth AML Directive²⁷ was adopted, further regulating the processing of personal data by FIUs²⁸ and increasing their capacity to cooperate.²⁹ For instance, the Directive sought to ensure timely and unrestricted access by FIUs to relevant financial data,³⁰ to empower FIUs to take urgent action³¹ and to improve coordination and cooperation between FIUs.³² Furthermore, the Directive required obliged entities to provide FIUs with *all necessary information*³³ and to hold a central register on their beneficial ownership to which FIUs and other competent authorities had access.³⁴ In addition, the Directive suggested that FIUs should *exchange information freely, spontaneously or upon request*, with third-country entities.³⁵

Only one year after the adoption of the Fourth AML Directive the Commission published, in response to the terrorist attacks in Paris and Brussels, and due to the ‘Panama Papers’ scandal,³⁶ amendments to that Directive in a proposal for a Fifth AML Directive.³⁷ The Fifth AML Directive,³⁸ which was adopted in May 2018,³⁹ seeks to strengthen the previous requirements concerning cooperation between na-

²⁷Directive (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 [2015] OJ L 141/73.

²⁸Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and the Council 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 Directive 2009/101/EC, SWD(2016) 223 final, Strasbourg, 5 July 2016, 6.

²⁹SWD (2017)275, 2, *supra* note 8.

³⁰Article 30(2) of Directive (EU) 2015/849.

³¹Article 32 (7) of Directive (EU) 2015/849.

³²Recital (54) of Directive (EU) 2015/849.

³³Article 33(1)(b) of Directive (EU) 2015/849.

³⁴Article 30(6) of Directive (EU) 2015/849.

³⁵Recital (54) of Directive (EU) 2015/849. In accordance with the recommendations of the Egmont Group, see: Egmont Group of Financial Intelligence Units Charter (July 2013) <https://egmontgroup.org/en/document-library/8>. This is seen as an internationally stated principle, see: A. Amicelle A., Chaudieu K. (2018) In Search of Transnational Financial Intelligence: Questioning Cooperation Between Financial Intelligence Units. In: King C., Walker C., Gurulé J. (eds) The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan, Cham, 652.

³⁶Will Fitzgibbon, ‘Five years later, Panama Papers still having a big impact’ (ICIJ, April 2021); <https://www.icij.org/investigations/panama-papers/five-years-later-panama-papers-still-having-a-big-impact/>.

³⁷Proposal for a Directive of the European Parliament and of the Council 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 Directive 2009/101/EC, COM(2016) 450 final, Strasbourg, 6 July 2016.

³⁸Directive (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.

³⁹Directive (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 L 156/43 as amended by Directive (EU) 2019/2177 of the European Parliament and of the Council of 18 December 2019 amending Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Directive 2014/65/EU on markets in financial instruments and Directive (EU)

tional authorities and to improve cross-border cooperation.⁴⁰ This includes a further enhancement of the effectiveness and efficiency of FIUs, for instance, by seeking to clarify the powers of and cooperation between them, as well as the abolishment of obstacles that may hinder the exchange of information between FIUs or the forwarding thereof.⁴¹ Under the Fifth AML Directive, FIUs are able to obtain information from any obliged entity, even where no prior STRs are filed.⁴² The amendments reinforce the preventive framework against money laundering, inter alia, by broadening the capacity of FIUs to access and exchange information.⁴³

In October 2018, a Directive on countering money laundering by criminal law⁴⁴ was adopted to complement the Fifth AML Directive.⁴⁵ Being based on Article 83(1) TFEU, that Directive⁴⁶ seeks to improve judicial cooperation in criminal matters and to reinforce the application of the Fifth AML Directive in order to tackle AML/CTF by means of criminal law.⁴⁷ In addition, a Directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences entered into force on 31 July 2019.⁴⁸ Besides new procedures for LEAs to obtain information from registered entities, the Directive seeks to extend the exchange of (financial) information to the broader scope of serious crime and provides for measures to facilitate access by FIUs to law enforcement information.⁴⁹ Being based on Article 87(2) TFEU,⁵⁰ the Directive seeks to enhance FIU cooperation by allowing FIUs of different Member States to exchange related to

2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing [2019] OJ L 334/115.

⁴⁰Ibid, 7. See also recital 16 of the amendments to Directive (EU) 2015/849.

⁴¹Thomas Wahl, '5th Anti-Money Laundering Directive', eucrim (20 October 2018).

⁴²Article 32(9) of Directive (EU) 2018/843.

⁴³Cf.: Maria Bergström, 'EU Anti-Money Laundering Regulation: Multilevel Cooperation of Public and Private Actors', in: *Crime Within the Area of Freedom, Security and Justice: A European Public Order* (Christina Eckes & Theodore Konstadinides eds., 2011).

⁴⁴Proposal for a Directive of the European Parliament and of the Council on countering money laundering by criminal law, COM(2016) 826 final, Brussels, 21 December 2016. This contribution refers to the most current version of the Council, which includes the amendments of the European Parliament after first reading, see Council Document 8450/19 of 15 May 2019.

⁴⁵'EU Adopts Tougher Rules on Money Laundering - Consilium,' accessed January 9, 2019, <https://www.consilium.europa.eu/en/press/press-releases/2018/10/11/new-rules-to-criminalise-money-laundering-activities-adopted/>.

⁴⁶Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law [2018] OJ L 284/22.

⁴⁷COM(2016) 826 final, recital 1.

⁴⁸Directive (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 [2019] OJ L 186/122.

⁴⁹Article 1(1) of Directive (EU) 2019/1153.

⁵⁰For the choice of legal basis, the Directive follows its predecessor, a Council Decision from 2000, in order to improve timely access and information exchange. See: Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [2000] OJ L 271/4.

terrorism or organised crime with their counterparts⁵¹ and to reply to requests for information by Europol, either through the national units or directly.⁵²

In December 2020, the European Data Protection Board (EDPB) issued a statement⁵³ on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, in which it emphasised the importance of AML measures to comply with the rights to privacy and data protection. Specifically, the Board referred to the rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU Charter), the principles of necessity and proportionality, as well as the case law of the Court of Justice of the European Union (CJEU).⁵⁴

Finally, in July 2021, the Commission proposed a legislative package to strengthen the EU's AML and CFT rules, which consists of four proposals. A proposal⁵⁵ to revise the Fifth AML Directive into a Sixth AML Directive, a proposal⁵⁶ for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, a proposal⁵⁷ on the revision of the 2015 Regulation on Transfers of Funds⁵⁸ and a proposal to establish an EU AML authority tasked with supervising and coordinating national authorities and private sector entities.⁵⁹

All instruments mentioned above, including the new AML Package, seek to contribute to the fight against money laundering and terrorist financing by establishing rules on better access to financial information and by facilitating the exchange of such

⁵¹ Articles 9 of Directive (EU) 2019/1153.

⁵² Article 12 of Directive (EU) 2019/1153.

⁵³ 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. In addition, the EDPB addressed a letter to the Commission European Commission on the upcoming review of the European AML/CFT framework. See: 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.

⁵⁴ 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.

⁵⁵ 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, Brussels, 20 July 2021.

⁵⁶ Laying down rules concerning: (a) the measures to be applied by obliged entities to prevent money laundering and terrorist financing; (b) beneficial ownership transparency requirements for legal entities and arrangements; (c) measures to limit the misuse of bearer instruments.

⁵⁷ Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), COM(2021) 422 final, Brussels, 10 July 2021.

⁵⁸ Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 [2015] OJ L 141/1.

⁵⁹ 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, Brussels, 20 July 2021.

information between different bodies.⁶⁰ However, while both the Fifth AML Directive as well as the proposed AML Package are based on Article 114 TFEU and solely address preventive efforts to support AML and CTF measures, both the Directive on countering money laundering by criminal law and the Directive on measures to facilitate law enforcement access to financial information find their legal bases under Title V TFEU.⁶¹

Hence, the wider regulatory AML framework shifted away from a predominantly single market focus to also include AML/CTF within the criminal law sphere.⁶² This may also imply consequences regarding the way in which personal data may be collected and exchanged. Thus, where AML/CTF legislative measures that also refer to FIUs find their legal bases under Article 87(2) TFEU, this might serve as an argument that FIUs may apply law enforcement data protection rules to their processing activities, namely the LED. The following sections will briefly present the different legal frameworks under the GDPR and the LED and subsequently propose arguments for and against the application of the LED to FIU processing operations.

3 Data Protection rules applicable to Financial Intelligence Units

FIUs are operationally independent and autonomous entities established in all EU Member States and are tasked with receiving (and, as permitted, requesting), analysing, and disseminating financial information, including personal data, via STRs.⁶³ Positioned between the private sector and LEAs, FIUs, acting as intermediaries, serve as the central reception point for receiving financial disclosures⁶⁴ from obliged entities.⁶⁵ Where, after the FIU analyses the material, there is a suspicion of money laundering or terrorist financing, the FIU shall forward the result of its analysis to the national authority responsible for prosecution.⁶⁶

In a nutshell, FIUs collect and process information for the purpose of analysing and identifying grounds to suspect money laundering, associated predicate offences

⁶⁰EPRS, 'Prevention of the use of the financial system for the purposes of money laundering or terrorist financing', PE 587.354, October 2016, 4. The first few financial intelligence units (FIUs) were established in the early 1990s.

⁶¹Explanatory Memorandum, COM(2018) 213 final, 2.

⁶²Bergström, 1164, *supra* note 26.

⁶³EPRS, 'Fighting tax crimes – Cooperation between Financial Intelligence Units', Ex-Post Impact Assessment, PE 598.603 (March 2017) 9.

⁶⁴Obliged entities are, according to Article 2 of the Third AML Directive, credit institutions; financial institutions; auditors, external accountants and tax advisors; notaries and other independent legal professionals; trust or company service providers; real estate agents; and other natural or legal persons trading in goods and casinos.

⁶⁵Recital 37 of 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 [2015] OJ L141/73. (Fourth AML Directive).

⁶⁶European Commission Fact Sheet, 'Preventing money laundering and terrorist financing across the EU. How does it work in practice?' https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf.

or terrorist financing. At a later stage, the results of their analyses and relevant information are disseminated to the competent LEAs.⁶⁷ Whereas EU AML legislation establishes the conditions and competence of FIUs to access the information needed for their analyses, details on collection and subsequent processing of that information are defined by the FIUs themselves.⁶⁸ This is supposed to guarantee the operational independence and autonomy of FIUs.⁶⁹

During the process of information gathering, FIUs may request information from their counterparts in other EU Member States. Since EU legislation does not require Member States to adopt specific structures according to which FIUs shall be organized, different national models have developed depending on the FIUs' functions, tasks, independence and domestic statuses.⁷⁰ These different models may be separated into administrative FIUs, law enforcement FIUs and mixed or hybrid FIUs.⁷¹ Although FIUs should exchange information with their foreign counterparts regardless of their respective model,⁷² obstacles regarding the access to, exchange and use of information as well as the operational cooperation exist due to the different national structures. While law enforcement FIUs normally obtain law enforcement competences, including the power to freeze transactions and seize assets,⁷³ administrative FIUs may be more restricted when processing personal data for their analyses. This leads to an information gap between different types of FIUs,⁷⁴ since law enforcement FIUs, on average, have better access to national police and judicial data⁷⁵ and may face limitations when cooperating with administrative FIUs in cross-border investigations.⁷⁶ The absence of a common structure to underpin this cooperation leads to situations where joint analyses are not performed for lack of common tools or resources. These divergences hamper cross-border cooperation, and thereby reduce the capacity to detect money laundering and terrorism financing early and effectively.⁷⁷

⁶⁷Eleni Kosta, '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' (30 July 2021) 25.

⁶⁸Ibid.

⁶⁹COM(2021) 421 final, 3.

⁷⁰SWD(2017) 275 final, 4, *supra* note 8.

⁷¹PE 587.354, October 2016, 38–39, *supra* note 56. There are similar typologies, for instance, the International Monetary Fund differentiates between four models: the administrative type FUI, the law enforcement type FUI, the judicial or prosecutorial FUI and the mixed or hybrid FUI. A similar typology has been adopted by the Egmont Group. See: Amicelle/Chaudieu, 664–665.

⁷²FATF Recommendations, 'International standards on combating money laundering and the financing of terrorism & proliferation' (2012–2018) 107.

⁷³In the EU, such LE-FIUs are existing in the UK and Estonia, see: World Bank Group, 'Module 2 – Role of the Financial Intelligence Units (incorporating peer reviewers comments)', p. 7, <http://pubdocs.worldbank.org/en/834721427730119379/AML-Module-2.pdf>.

⁷⁴EPRS, 'Fighting tax crimes – Cooperation between Financial Intelligence Units, Ex-Post Impact Assessment', PE 598.603 (March 2017) 39.

⁷⁵Project 'Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy – ECOLEF' (funded by the European Commission – DG Home Affairs, JLS/2009/ISEC/AG/087), Final Report, February 2013.

⁷⁶SWD(2017) 275 final, 5.

⁷⁷COM(2021) 421 final, 3.

Hence, the distinction into different FIU models may have an impact on the way in which the different FIUs may process information for their analyses.⁷⁸ Since the analysis by FIUs involves the processing of personal data, such processing operations must comply with the EU data protection *acquis*. While the GDPR is applicable to general processing activities by both public and private entities, the LED solely applies when both, its personal and material scope are satisfied, namely where a competent authority within the definition of Article 3(7) LED⁷⁹ (personal scope) processes personal data for law enforcement purposes (material scope).⁸⁰ In the law enforcement context, competent authorities may generally process personal data more flexibly, as transparency obligations of controllers are less rigid and data subject rights to information and access may be restricted more easily in order not to jeopardize ongoing investigations.

Whereas the FIU model might not be the predominant factor in determining the applicable data protection framework, it influences the way in which FIUs may process and exchange information and the types of analyses that they are authorized to carry out. Hence, where law enforcement FIUs are permitted to process law enforcement information, it could be argued that such processing falls within the material scope of the LED. On the other hand, administrative FIUs that do not have access to such types of information fulfil neither the personal nor the material scope of the Directive. Whereas the processing by administrative FIUs of non-law enforcement information is governed by the rules under the GDPR's data protection regime, FIUs that may process law enforcement information could in many occasions process personal data and apply the LED, as in many Member States, the material scope of the Directive defines its personal scope.

4 GDPR or LED?

Whereas some authors as well as many of the FIUs themselves naturally assume the applicability of the LED to their processing activities,⁸¹ other scholars – particularly those coming from the data protection field – are more careful in such assumptions.⁸²

⁷⁸Commission Staff Working Document, 'On improving cooperation between EU Financial Intelligence Units', SWD(2017) 275 final, Brussels, 26 June 2017, 6.

⁷⁹Article 3(7) LED defines a competent authority as (a) any public authority competent for 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; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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.

⁸⁰For 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, Article 1(1) of Directive (EU) 2016/680.

⁸¹See, for instance, Jean-Baptiste Maillart, 'The Anti-Money Laundering Architecture of the European Union' in: Benjamin Vogel and Jean-Baptiste Maillart (eds.) *National and International Anti-money Laundering Law – Developing the Architecture of Criminal Justice, Regulation and Data Protection* (2020 Intersentia) 126.

⁸²Eleni Kosta writes that '[...] 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

The following section shall first provide examples in favour of an application of the LED to the processing of personal data by FIUs and subsequently propose arguments against such application.

4.1 Arguments in favour of an application of the LED to FIU processing

FIUs often do not merely provide expertise to LEAs but rather analyse complex patterns of transactions on their own and thereby add value to the collected information.⁸³ Furthermore, the EU legislator left it to the national level to determine the exact functions and reporting systems of FIUs,⁸⁴ which led to divergences regarding the relationship between obliged entities, FIUs and LEAs in the different EU Member States.⁸⁵ Where Member States opted to confer real investigative and prosecutorial powers to their national FIUs, those could be seen as forming part of the LEAs themselves and therefore, eligible to apply the data protection rules under the LED.

FIUs are established pursuant to Article 32 of the Fifth AML Directive (EU) and, for the time being, Article 17 of the proposed Sixth AML Directive.⁸⁶ The main tasks of the FIU under paragraph one of both the current and the proposed provision are to prevent, detect and effectively combat money laundering and terrorist financing. Under Article 18(1)(c) of the proposed Directive, FIUs, for the purpose of their operational analyses, shall have direct or indirect access law enforcement information.⁸⁷ Hence, FIUs would have direct access to the databases held by the national police and/or intelligence agencies in order to subsequently use those data for their analyses.⁸⁸ Such analytical processing of law enforcement information for the purpose of preventing, detecting and effectively combating money laundering and terrorist financing should suffice to satisfy the material scope of the LED. As mentioned above, in many Member States, the material scope may define the personal scope of the LED, and hence, where FIUs – even if they would not be regarded as competent authorities under the LED – would process personal data for the above purposes, this could lead to the application of the LED.

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'. See: Kosta (n. 83).

⁸³Magdalena Brewczynska, 'Financial Intelligence Units: Reflections on the applicable data protection legal framework', *Computer Law & Security Review* (2021) 43, 13.

⁸⁴Valsamis Mitsilegas, *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance versus Fundamental Legal Principles* (Kluwer Law International 2003), 155.

⁸⁵Valsamis Mitsilegas, *EU Criminal Law: EU Criminal Law* (Bloomsbury Publishing Plc 2009), 43.

⁸⁶Article 2(3) of Directive (EU) 2019/1153.

⁸⁷Such information includes any type of information or data which is already held by competent authorities in the context of preventing, detecting, investigating or prosecuting criminal offences and any type of information or data which is held by public authorities or by private entities in the context of preventing, detecting, investigating or prosecuting criminal offences and which is available to competent authorities without the taking of coercive measures under national law.

⁸⁸The 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. See Kosta, (n.68) 6.

In numerous Member States FIUs are regarded as competent authorities, which in return means that both personal scope and material scope of the LED are satisfied. In those Member States where the FIUs are law enforcement-type FIUs, they normally also have law enforcement powers and are positioned within the structure of the national LEA. In those countries, the FIU commonly applies the LED to its processing activities. This is, for instance, the case in Denmark or Luxembourg where the FIU is part of the State Prosecutor's office, or in Finland, where the FIU is located within the overall structure of the Finnish Police. In Germany, the FIU is of law enforcement type, although it forms part of the Federal Customs office. This classification might be due to the fact that initially, the FIU was established in the Federal Criminal Police Office.⁸⁹ Similarly, the FIUs in Belgium, Estonia and the Netherlands, which are nowadays self-standing authorities, but nevertheless classified as law enforcement type FIUs, were previously established within the structure of the national Police. This might explain why all of the above FIUs apply the LED to their processing activities.

In addition, both the current as well as the proposed legal framework on AML/CTF measures are anything but unambiguous when it comes to a clear definition of whether or not FIUs may apply the LED. Although FIUs are currently established and regulated under the Fifth AML Directive,⁹⁰ which derives from an internal market legal basis, that Directive ultimately refers to the processing of personal data by obliged entities, which are subject to the rules under the GDPR, as recognized in Article 41 of the Directive. Hence, while that provision *does* state that the GDPR generally applies to processing carried out under the Fifth AML Directive, it only refers to obliged entities, while not mentioning FIUs.

The Directive on rules to facilitate access by competent authorities to financial and other information is supposed to compensate for the limitations of the internal market legal basis and to tackle existing problems in the area of police cooperation.⁹¹ That Directive repeals a Council Decision⁹² on cooperation between FIUs, which was adopted at a time when the domestic processing of personal data by competent authorities *within* the Member States was not regulated by EU law. That Council Decision makes reference to CoE instruments, namely Convention 108⁹³ and Recommendation R (87) 15 on regulating the use of personal data in the police sector.⁹⁴ It could, therefore, be argued that, since the Council Decision does not mention the

⁸⁹See 2015 Annual report of the German FIU; <https://www.bka.de/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/FIU/fiuJahresbericht2015Englisch.html?sessionId=371246CD1E603275498BF7157CDD4DC6.live301>.

⁹⁰SWD(2018) 114 final, 24.

⁹¹SWD(2018) 114 final, 24.

⁹²Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information [2000] OJ L 271/4.

⁹³Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108. The Convention entered into force on 1 October 1985.

⁹⁴Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulation the use of Personal Data in the Police Sector, 17 September 1987.

Directive 95/46/EC,⁹⁵ processing by FIUs was considered law enforcement processing.

Under Article 18 of the Directive on rules to facilitate access by competent authorities to financial and other information, data subject rights may be restricted in accordance with the respective rules under the GDPR and the LED. It is, however, unclear under which of both instruments FIUs are allowed to process personal data for the performance of their tasks. On that background, Articles 8⁹⁶ and 9⁹⁷ of the Directive clearly refer to law enforcement data that are to be exchanged between FIUs and competent authorities, as well as among the FIUs in different Member States. Although both Articles explicitly differentiate between ‘FIUs’ and ‘competent authorities’, the *exchange of information for the prevention, detection and combating of money laundering and associate predicate offences* or the *analysis of information related to terrorism or organised crime associated with terrorism* could be seen as processing carried out for law enforcement purposes. In those situations where FIUs would process such law enforcement information, they could apply the LED, even if they do not satisfy the personal scope, simply by extending the latter via the material scope.

Another provision under the Directive on law enforcement access to financial and other information that could support the argument that FIUs might be considered competent authorities under the LED, is Article 7(5).⁹⁸ While that provision distinguishes competent authorities from FIUs, the second part of that paragraph could nevertheless be interpreted as including FIUs within the definition of competent authorities within the personal scope of the LED. That section refers to the processing of personal data for law enforcement purposes ‘other than those for which the personal data are collected in accordance with Article 4(2) [of the Directive]’. Article 4(2) LED thus regulates the subsequent processing of personal data under the Directive, which can only take place where these data have previously been processed by a competent authority within the scope of Article 4(1). Because of the ambiguous wording of Article 7(5) of the Directive on law enforcement access to financial information, FIUs could represent competent authorities within the meaning of Article 4(1) LED and would thus, fall within the personal scope of the Directive.⁹⁹

It is regrettable that the proposed AML Package does little to nothing to provide some clarity on the data protection framework applicable to FIU processing. It could even be argued that some of the legislative proposals might lead to even more ambiguity. For instance, Article 2(31)(a) of the proposed Regulation on the prevention

⁹⁵Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

⁹⁶Requests of information by a FIU to competent authorities.

⁹⁷Exchange of information between FIUs in different EU Member States.

⁹⁸Requests for information by competent authorities to an FIU.

⁹⁹It must, however be noted that this provision has been interpreted in a way that Article 4(2) should be seen as subsequent processing of GDPR data. Hence, where data that has previously been processed by an FIU within the scope of the GDPR, Article 4(2) LED would be the legal basis for the subsequent use of GDPR data for law enforcement purposes. See: for a different interpretation see: Catherine Jasserand, ‘Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?’ (March 1, 2018). European Data Protection Law Review, Vol. 4 (2018), Issue 2, pp. 152-167.

of the use of the financial system for the purposes of money laundering or terrorist financing defines FIUs as competent authorities.¹⁰⁰ Furthermore that article defines supervisory authorities, public authorities with designated responsibilities for combating money laundering or terrorist financing and public authorities that have the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that has the function of tracing, seizing or freezing and confiscating criminal assets as competent authorities. Thus, the provision neither includes traditional LEAs within the definition of competent authorities, nor does it use the wording under Article 3(7) LED. This might not only lead to textual inconsistencies, but also trigger confusion with regard to the question what/who constitutes a competent authority and may ultimately apply the LED.

Finally, some rules under the LED itself could serve to argue in favour of an application of the Directive to the processing of personal data by FIUs, as providing more suitable safeguards. This might, for instance, be the case with regard to the categorization of data subjects, the requirement to classify personal data into information based on facts and information based on personal assessments under Articles 6 and 7 of the LED, or the obligation to keep logs of certain processing operations pursuant to Article 25 LED. Those provisions are non-existent under the GDPR and might, in fact, contribute to higher protection standards in certain processing situations.¹⁰¹ In addition, it could be argued that the system on the restriction of data subject rights under the LED is more developed than the one under the GDPR, despite the latter's strong transparency obligations:

Article 39(1) of the Fifth AML Directive includes a rather broad non-disclosure clause that applies where obliged entities shall refrain from informing their customers if money laundering or terrorist financing analyses are being carried out. The non-disclosure obligation also applies to guarantee that inquiries, analyses, investigations or procedures for AML purposes are not obstructed and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.¹⁰² In those cases, obliged entities would rely on Article 23 GDPR, which allows for the restriction of data subject rights and corresponding data protection principles by way of legislative measure.

Article 23 GDPR represents a horizontal limitation clause on the restriction of data subject rights for a number of grounds.¹⁰³ The LED on the other hand incorporates a structure pursuant to which the restriction of each right requires a specific legal basis.

¹⁰⁰ Article 2(31)(a) of COM (2021) 420 final.

¹⁰¹ On this, see Teresa Quintel, 'Follow the Money, If You Can - Possible Solutions for Enhanced FIU Cooperation Under Improved Data Protection Rules' *Europarättslig Tidskrift* 1/2019 (2019).

¹⁰² Article 41(4)(b) of Directive (EU) 2019/2177.

¹⁰³ Data protection principles and data subject rights may be restricted in order to safeguard: (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 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)

Hence, while Article 23 GDPR could be regarded as general limitation clause, the system allowing for restrictions of data subject rights under the LED is laid down in individual derogation clauses that follow each right enshrined in the Directive. Under the LED, the national legislator may adopt legislative measures to restrict the individual data subject rights laid down in Article 13 LED (right to information), Article 14 LED (right of access) and Article 16 LED (right to rectification and erasure). Article 13(3) LED, Article 15 LED and Article 16(4) LED each include an option to restrict these rights separately for as long as necessary and proportionate. In addition, these provisions entail clear instructions for the controller to inform data subjects of any restriction as well as the corresponding processing that was carried out about them as soon as such notification may no longer jeopardize ongoing investigations. Although the GDPR is based on strong transparency obligations towards data subject, its system on the restriction of data subject rights lacks such specific provisions that would compel controllers to inform data subjects after a restriction has taken place. Admittedly, the provisions under the LED includes qualifiers such as the wording *for as long as such a [...] restriction constitutes a necessary and proportionate measure*.¹⁰⁴ Yet, the accountability obligation that also applies under the Directive would require any restriction to be justifiable before the supervisory authority.

In addition, the Directive provides, under its Article 17, for an important administrative remedy by availing individuals the possibility to have their rights exercised by the national data protection supervisory authority on their behalf. In those circumstances, the LED might in fact constitute a more suitable instrument in order to allow for both, effective cooperation between obliged entities, FIUs and other LEAs, while at the same time, ensure the notification or indirect access rights for data subjects.

The EU legislator, by leaving the LED's scope extremely broad, assigned the task of determining which authorities may apply the Directive to the national level. Consequently, it is left to the national legislators to define whether FIUs fall within the personal scope of the LED. In addition, under many national transposition acts, the Directive's material scope may define its personal scope, so that authorities which process personal data for law enforcement purposes may apply the LED to their processing operations, albeit not being LEAs per se.¹⁰⁵

In addition, numerous Member States include a wide range of processing activities within 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*. This often means that the Directive may apply to processing activities that are by far less of a law enforcement nature than the processing of personal data by FIUs. This is, for instance, the case in the field of migration management or border control. When comparing these two areas, the application of

and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims.

¹⁰⁴Under Article 13(3) LED, information to the data subject in specific cases may be delayed, restricted or omitted, under Article 15 LED the right of access may be restricted and under Article 16(4) LED, information to the data subject about refusals for rectification or erasure may be restricted *for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned*.

¹⁰⁵This is, for instance, the case in Germany.

the LED to FIU processing when countering money laundering or terrorist financing might be more justifiable than the Directive's application where border guards check the identity of so-called third country nationals. Such argument might not provide a legal ground for the LED's application to FIUs, but it demonstrates that in reality, Member States included more authorities within the Directive's scope than initially anticipated.¹⁰⁶ In order to prevent such broad application of the LED's scope, legislative amendments might prove necessary.

4.2 Arguments against the application of the LED to FIU processing

Both the current AML/CTF legal framework as well as the proposed AML Package are not only established on an internal market legal basis, but also explicitly refer to the GDPR¹⁰⁷ as applicable instrument to the processing of personal data¹⁰⁸ and distinguish between FIUs and competent authorities.¹⁰⁹ Notice should also be taken of Article 95 GDPR, which states that Directive 95/46/EC is repealed by the GDPR, but all the references to the repealed Directive will be interpreted as references to the GDPR. With regard to FIUs, this means that all references to Directive 95/46/EC in the previous AML regime became references to the GDPR.

In addition, the fact that the Directive on law enforcement access to financial information makes a difference between FIUs and LEAs should be taken into account. The separation between administrative and law enforcement authorities should be put into a wider perspective, also considering existing structures. Such differentiation is, for instance, the case with regard to EU Agencies, where the law distinguishes between Agencies that are competent for administrative offences and Agencies that are competent for criminal offences, as is the case for Olaf (the European Anti-Fraud Office) and the EPPO (the European Public Prosecutor's Office).

In addition, FIUs have a different applicable legal regime than so-called Passenger Information Units (PIUs), which collect passenger name record (PNR) data¹¹⁰ from air carriers, to store, process and transfer those data or the result of their processing to the competent authorities.¹¹¹ PIUs are generally established within the organizational structure of the competent LEAs in the Member States and themselves competent for the prevention, detection, investigation or prosecution of terrorist offences and of

¹⁰⁶Declaration 21 attached to the Lisbon Treaty only refers to particular rules on the protection of personal data and the free movement of such data *in the fields of judicial cooperation in criminal matters and police cooperation* that may prove necessary because of the specific nature of these fields.

¹⁰⁷It refers to Directive 95/46/EC, the predecessor of the GDPR.

¹⁰⁸Recital 38 of the Fifth AML Directive puts forward that data subjects should be informed in accordance with the provisions of the GDPR. Yet, that recital also makes reference to the LED, without clarifying in which circumstances it would apply and whether it could also be used by FIUs.

¹⁰⁹See, for instance, Article 30(5)(a), Article 32(3) or Recital 39 of Directive (EU) 2015/849.

¹¹⁰Such as the dates of travel and travel itinerary, the ticket information, contact details like address and phone number of the travelling person, travel agent, payment information or seat number and baggage information.

¹¹¹Article 4(2)(a) of Directive (EU) 2016/681.

serious crime.¹¹² Under the PNR Directive,¹¹³ PIUs are subject to the rules of the LED.¹¹⁴

Against that background, Article 17(4) of the proposed Sixth AML Directive states that in cases where a FIU is located within the existing structure of another authority, the FIU's core functions shall be independent and operationally separated from the functions of the host authority. Hence, the provision not only differentiates between FIUs and other (law enforcement) authorities, but also between their tasks and thus, processing activities, which should have an impact on the applicable data protection regime. In that vein, it needs to be noted that some FIUs do not even analyse the data that they receive and only operate databases that are directly accessible for LEAs. In such cases, it can hardly be argued that the FIU itself processes personal data for law enforcement purposes and would be capable of applying the LED to manage a police database.

In addition, even where law enforcement FIUs may apply the Directive to their processing operations, Article 9 LED stipulates that where competent authorities process personal data for non-law enforcement purposes, the GDPR applies to their processing activities. Paragraphs 1 and 2 of that Article clearly state that the GDPR is applicable whenever competent authorities process personal data for purposes other than for the prevention, investigation, detection or prosecution of criminal offences, unless such processing is not regulated by EU law.¹¹⁵ In those Member States where FIUs may process personal data within the scope of the LED, their tasks should be explicitly clarified in order to prevent grey zones between the GDPR and the LED and to ensure that their FIU's non-law enforcement processing falls within the scope of the GDPR.

5 Data retention and data retention: comparing standards

One area that has not (yet) been taken into consideration, but which nevertheless deserves to be taken into account for the sake of this analysis is the area of data retention. With financial data, it is possible to accurately conclude on the shopping behavior of a purchaser, his or her personal choices, to determine time of a purchase and his or her exact location, as payments are easily traceable. Due to the long retention periods and the potential re-use of financial information for law enforcement purposes, this aspect should play an important role in the discussion on data retention schemes, also considering the CJEU's case law on that matter.

¹¹²Article 4(1) of Directive (EU) 2016/681.

¹¹³Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

¹¹⁴Article 13 of Directive (EU) 2016/681.

¹¹⁵For instance, the processing carried out by national intelligence agencies or military services for purposes of national security, see Article 2(3)(a) LED. Neither the GDPR nor the LED apply when personal data are processed by Union institutions and bodies, in which case Regulation (EU) 2018/1725 applies; or, where the specific instruments of EU Agencies such as Europol are applicable.

In the area of data retention, access to personal data by law enforcement authorities and the issue of mass surveillance by intelligence agencies, there important cases have been decided especially during the last couple of years.¹¹⁶ On EU level, the CJEU has progressively strengthened data subjects' rights through its case law,¹¹⁷ in particular, since the Lisbon Treaty of 2009 converted the EU Charter into a legally binding instrument of EU primary law, progressively serving as basis for the CJEU's interpretation of fundamental rights. Previously, the Court had been dependent on referring to fundamental rights as general principles of EU law and Article 8 European Convention on Human Rights (ECHR) in its jurisprudence.¹¹⁸

However, until recently, the most prominent CJEU cases on data retention measures by private entities almost exclusively dealt with the retention of telecommunications data. Hence, there is a need to evaluate the CJEU judgments on data retention not solely in relation to the retention of telecommunications data, but to apply the Court's findings also to other data retention regimes on EU level. In that regard, the regime on the retention of financial data should be assessed concerning its (in)compatibility with the standards set by the jurisprudence of the CJEU and the European Court of Human Rights (ECtHR).

Under the Fifth AML Directive, Member State law shall determine the period in which financial data should be retained by obliged entities.¹¹⁹ Generally, that retention period should be fixed at five years after the end of a business relationship or of an occasional transaction. When justified and where deemed useful for the purposes of prevention, detection or investigation of money laundering and terrorist financing, such information may be retained for an additional five years, in line with the necessity and proportionality requirements.¹²⁰

Similarly, under the proposed Sixth AML Directive, obliged entities would have to retain a copy of the documents and information obtained in the performance of the customer due diligence and supporting evidence obligations as well as records of

¹¹⁶See for instance Joined Cases C-293/ 12 and C-594/ 12, *Digital Rights Ireland Ltd* (C-293/ 12) and *Seitlinger* (C-594/ 12) (CJEU, 8 April 2014) ECLI:EU:C:2014:238; Joined Cases C-203/ 15 and C-698/ 15 *Tele2 Sverige AB* (C-203/ 15) and *Watson* (C-698/ 15) (CJEU, 21 December 2016) ECLI:EU:C:2016:970 and with regard to ECtHR cases *Roman Zakharov v Russia* App no 47143/ 06 (ECtHR, 4 December 2015) and *Szabó and Vissy v Hungary* App no 37138/ 14 (ECtHR, 12 January 2016) as well as earlier *Kennedy v. the United Kingdom* App no 26839/ 05 (ECtHR, 18 May 2010).

¹¹⁷Cases concerned with data retention and mass surveillance, see: Case C-301/ 06 *Ireland v European Parliament and Council*, (CJEU, 10 February 2009) ECLI:EU:C:2009:68; Joined Cases C-293/ 12 and C-594/ 12, *Digital Rights Ireland Ltd* (C 293/ 12) and *Seitlinger* (C-594/ 12) (CJEU, 8 April 2014) ECLI:EU:C:2014:238; Case C-362/ 14, *Schrems* (CJEU, 6 October 2015) ECLI:EU:C:2015:650; Joined Cases C-203/ 15 and C-698/ 15 *Tele2 Sverige AB* (C-203/ 15) and *Watson* (C-698/ 15) (CJEU, 21 December 2016) ECLI:EU:C:2016:970; *Opinion 1/15* on the Draft PNR Agreement between the EU and the US, ECLI:EU:C:2017:592, 26 July 2017; CJEU, Case C-311/ 18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, ECLI:EU:C:2020:559, 16 July 2020; CJEU, Joined Cases C-511/18, C-512/ 18 and C-520/ 18, *la Quadrature du Net*, ECLI:EU:C:2020:791, 6 October 2020.

¹¹⁸E.g. Case C-465/ 00 and C-138/ 01 *Rechnungshof v ORF* (CJEU, 20 May 2003) ECLI:EU:C:2003:294, para. 70 et seq.

¹¹⁹Article 40(1) of Directive (EU) 2015/849.

¹²⁰Recital 44 of Directive (EU) 2015/849.

transactions for five years.¹²¹ In addition, Member States could allow or require the retention of such information or documents for a further period of five years.¹²²

While the ECtHR has, on several occasions,¹²³ decided on the retention of financial data, CJEU case law on that matter is overdue, despite the Court's rich case law on data retention measures applicable in the case of telecommunication data. Three years after the entry into application of the GDPR and seven years after the Court's first landmark judgment on the retention of telecommunications data,¹²⁴ a case on the long storage times of financial data is still lacking.

On 19 October 2021, the Grand Chamber of the CJEU deliberated whether the public register of beneficial owners under the current AML framework would be in conformity with the rights to privacy and data protection. The case is about the requirement for Member States to set up a central register containing information on the beneficial ownership of corporate and other legal entities under the Fifth AML Directive. In the case that was brought by a Luxembourgish court, it was argued that the requirement to make this register accessible to any member of the public is too excessive.¹²⁵ Unfortunately, the question on data retention periods applicable to financial data was not a matter in this case. However, it will be interesting to see how the Court will decide on that matter in the future.

6 Further outlook and concluding remarks

Ultimately, the harmonized rules under the LED could ensure an adequate level of data protection while, at the same time, ensuring smooth cooperation between FIUs and (other) competent authorities. Allowing FIUs to gather, analyse and exchange information more flexibly might improve the effectiveness of their cooperation and could help maintaining their role as intermediary between the private sector and LEAs. In addition, an enhanced effectiveness of FIUs might serve as an argument against further possibilities of LEAs to directly access personal data.

It is important to repeat that, in many Member States, the LED is being applied in situations that seem by far less of a law enforcement nature than the processing of personal data by FIUs. For instance, in the context of border control and the irregular entry of so-called third country nationals, many national legislators allowed, by criminalizing such irregular entry, the application of the LED in such situations. This is even the case where authorities such as border guards would otherwise not be competent authorities within the scope of the Directive. It could, therefore, be argued

¹²¹Article 56(3) of COM(2021)420.

¹²²where the necessity and proportionality of such further retention have been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing Article 56(4) of COM(2021) 420.

¹²³*M.N. and others v. San Marino* App no 28005/ 12 (ECtHR, 7 October 2015), *Brito Ferrinho Bexiga Villa-Nova v. Portugal* App no 69436/ 10 (ECtHR, 1 December 2015) or *Sommer v. Germany* App no 73607/ 13 (ECtHR, 27 April 2017).

¹²⁴*Digital Rights Ireland*.

¹²⁵CJEU, C-601/ 20, request for a preliminary ruling, 13 November 2020.

that if the LED applies in such situations, it should also be applicable with regard to AML/CTF processing carried out by FIUs.

The processing of personal data by FIUs within the scope of the LED might, in the future even bring certain data protection benefits. With regard to the recently proposed AI Act,¹²⁶ the latter excludes from its scope certain high-risk processing operations carried out by LEAs. Banks and non-law enforcement authorities on the other hand might have more possibilities to engage in such AI-enabled processing operations. Evidently, there will be many loopholes to also allow LEAs to circumvent the abovementioned exceptions. Nevertheless, the threshold might be more difficult to establish.

The recently proposed AML Package, consisting of two new regulations, a new AML Directive, and a proposal for the revision of an already existing Regulation on the transfer of funds, will need to be assessed in more detail, also with regard to the data protection rules applicable to FIUs. As it stands now, the proposed framework adds little to clarify whether FIUs could apply the LED to their processing activities. Therefore, it would be welcome if the negotiations would further clarify this issue.

In addition, the reform proposes a Regulation establishing an Authority on AML and CTF measures (AMLA). The new Authority would be responsible for both directly supervising some of the Union's largest financial players as well as aiding and monitoring national FIUs. In addition, AMLA would assume some of the tasks carried out by already existing EU agencies.¹²⁷ This would include taking over the management of the secure communication network between FIUs, previously maintained by Europol.¹²⁸ Which data protection rules would apply to this new EU Agency where it will process law enforcement information remains to be seen. Yet, there is a risk that AMLA will be able to argue that it should fall within the scope of Chapter IX of Regulation (EU) 2018/1725 that governs the processing of so-called operational personal data (law enforcement personal data). This would be problematic, as Chapter IX remained unfinished with regard to rules on international transfers and supervision by the European Data Protection Supervisor.¹²⁹

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

¹²⁶Proposal for a Regulation of the European Parliament and of the Council Laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, Brussels, 21 April 2021.

¹²⁷Sotiris Paphitis, 'The EU's AML Package: an examination', European Law Blog (October 2021); <https://europeanlawblog.eu/2021/10/12/7922/>.

¹²⁸In the end of 2019, the European Data Protection Supervisor set an end to FIU.net because of a lack of legal basis for Europol to organize such a network.

¹²⁹On Chapter IX, see Teresa Quintel, 'Managing Migration Flows by Processing Personal Data Within the Adequate Data Protection Instrument - scoping exercise between general and law enforcement data protection rules applicable to third country nationals, doctoral thesis defended on 10 September 2021.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.