Faculty of Law,
Economics
and Finance

**Law Working Paper Series**
Paper number 2019-001

# Follow the Money, if you can

## Possible solutions for enhanced FIU cooperation under improved data protection rules

Teresa Quintel, University of Luxembourg, Uppsala University
teresa.quintel@uni.lu

18/01/2019

UNIVERSITÉ DU LUXEMBOURG

# Follow the Money, if you can

## Possible solutions for enhanced FIU cooperation under improved data protection rules

**Abstract**

Financial information can play a key role in tackling Money Laundering (ML), Terrorist Financing (TF) and combatting serious crime more generally. Preventing and fighting ML and the financing of terrorism were top priorities of the European Agenda on Security, which might explain the fast developments regarding the regulation of Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF).

During the past years, the European Commission (Commission) proposed several legal texts to reform the current AML framework and to facilitate timely law enforcement (LE) access to financial data for the prevention, detection, investigation and prosecution of serious crime. The line between administrative sanctions and criminal law measures seems to become increasingly blurred, as the latest proposals are no longer based on an internal market provision, but on police and judicial cooperation legal bases.

Financial Intelligence Units (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). Because of the international nature of financial crime, cooperation between FIUs is of paramount importance. Yet, due to different organizational settings in the EU Member States, FIUs are not always able to exchange data effectively, which leads to information gaps.

One of the reasons why the data exchange between FIUs is impeded are data protection rules that apply differently depending on the organizational structure of the FIUs in the 28 Member States. Whereas some FIUs must adhere to the stricter data protection rules under the General Data Protection Regulation (GDPR), others may exchange data more flexibly within the scope of the data protection Directive for police and criminal justice authorities (LED). Therefore, the counter-argument to granting broader LE-access rights to financial data by LEAs could be to enable a more effective exchange of data between FIUs.

This article argues that FIUs should be able to process personal data within the scope of the LED, in order to have more flexibility to receive, analyse and exchange data: On the one hand, the LED provides sufficiently high data protection standards and adequate safeguards for data subjects while allowing FIUs to carry out their tasks effectively under harmonized rules. On the other hand, this would be an argument to strengthening the role of FIUs as neutral intermediaries instead of granting additional access to personal data by LEAs.

**Key Words:** FIUs, Anti Money Laundering, Terrorist Financing, Data Protection, GDPR, LED.

## I. Introduction

Terrorist and organized crime networks 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.[2] Financial information is therefore a crucial tool for the identification of criminal networks and for the prevention, detection, investigation and prosecution of serious crime and terrorism.

[1] 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.

[2] Proposal 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.

Financial (personal) data are most commonly held by banks, but also by other private entities such as auditors, real estate agents, tax advisors, trusts or casinos. These regulated entities are required to compile financial transactions that are suspected to facilitate ML or TF in so-called suspicious transaction reports (STRs).[3]

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.[4] Positioned between the private sector and LEAs, FIUs, acting as intermediaries, serve as the central reception point for receiving financial disclosures[5] from obliged entities.[6] Where, after the FIU analyses the material, there is a suspicion of ML or TF, the FIU shall forward the result of the analysis to the national authority responsible for prosecution.[7]

Because of the divergent systems in the Member States, FIUs may be considered administrative authorities in some Member States, while being regarded LE-FIUs in others. This distinction in different FIU types may also have an impact on the way the different FIUs may process information for their analyses.[8]

Since the analysis by FIUs involves the processing of personal data, such processing operations must comply with the EU data protection *acquis*. In May 2018, the EU Data Protection Reform[9], consisting of the GDPR[10] and a Directive[11] establishing rules for the protection of individuals with regard to the processing of personal data by competent authorities for purposes of LE, came into force.

While the GDPR is applicable to general processing activities by both public and private entities, the LED solely applies where a competent authority within the definition of Article 3(7) LED[12] processes personal data for LE-purposes.[13] In the LE-context, competent authorities may generally process personal data more flexibly, as transparency obligations of controllers are less rigid and data subjects rights of access and information may be restricted more easily in order not to jeopardize ongoing

[3] European Parliamentary Research Service (EPRS), 'LE-access to financial data', PE 615.665 (April 2018) 2.
[4] EPRS, 'Fighting tax crimes – Cooperation between Financial Intelligence Units', Ex-Post Impact Assessment, PE 598.603 (March 2017) 9.
[5] Obliged 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.
[6] Recital 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).
[7] European 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.
[8] Commission Staff Working Document, 'On improving cooperation between EU Financial Intelligence Units', SWD(2017) 275 final, Brussels, 26 June 2017, 6.
[9] '2018 Reform of EU Data Protection Rules', Text, European Commission - European Commission, accessed May 9, 2018, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ, L 119/1.
[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119/ 89.
[12] Article 3(7) 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.
[13] 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.

investigations. Consequently, in Member States where national FIUs are considered competent authorities within the meaning of the LED, the collection, analysis and exchange of personal data with other FIUS and competent authorities is less restricted than in Member States where the processing of FIUs falls within the scope of the GDPR. The applicability of data protection rules along the type of FIUs, however, might seem misleading, as firstly, all FIUs could be considered competent authorities within the scope of the LED and secondly, the respective data protection instrument should apply in accordance with the purposes of the processing.[14]

This article illustrates the benefits for FIU cooperation where the processing of personal data is carried out within the scope of the LED. It shall be argued that, although under the LED data protection rights may be restricted easier than under the GDPR, the Directive provides an adequate level of fundamental rights protection while facilitating the exchange of personal data between FIUs, as they will be able to rely on uniform data protection rules. The GDPR would remain applicable to the processing of data for non-LE purposes.[15] On the one hand, this could help reduce the gaps that FIUs experience when sharing information amongst each other. On the other hand, this would be an argument against the broadening of LE-access to personal data, as FIUs would be able carry out their role as 'neutral intermediary' more effectively.

The following section will give a broad overview of how AML/CTF regulation in the EU developed during recent years and illustrate the different FIU models as well as the shortcomings regarding FIU cooperation within the EU in Section II.1. Thereafter, Section III will briefly outline the EU Data Protection Reform, and demonstrate the improvements that came into force with the LED (Section III.1). Section IV suggests adopting an approach to facilitate the exchange of personal data between FIUs by applying the LED whenever processing is carried out for LE-purposes. That section also points to the concerns that remain under the proposed approach, emphasising the increasingly blurred line between administrative and criminal law measures and the issues that arise were additional purposes are added to process personal data in relation to AML and CTF.

## II. Anti-Money Laundering and Counter Terrorist Financing in the European Union

The EU legal regime on ML and TF has been developed since the 1990s and has progressively strengthened the role of FIUs.[16] The First AML Directive was adopted in 1991[17] 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.[18] The provisions of that Directive were refined in the Second[19] and the Third AML

[14] In practice this would mean that, although FIUs would be considered competent authorities within the scope of the LED, they would still have to process personal data within the scope of the GDPR as long as their processing would not be for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
[15] According to the World Bank's 2018 Report on FIU cooperation with LEAs, a very high number of FIUs (70 percent) reported that they may disseminate information to competent authorities when they suspect that an administrative offence was committed. Some respondent LEAs (15 percent) mentioned that they are also recipients of such information. Moreover, 13 percent of the FIUs reported that they receive LEA requests that are not crime-related. Thus, in EU Member States where such offences do not fall within the scope of the LED (see recital 12 LED on the very broad definition of criminal offences that may be included within the scope of the LED), the GDPR would apply to the processing of information concerning administrative offences by FIUs as well as by LEAs (despite that fact that such practices may lead to an improper use of FIU powers). See: K. Stroligo, C.L. Hsu and T. Kouts, 'Financial Intelligence Units Working With LEAs and Prosecutors' (2018), 8. https://star.worldbank.org/sites/star/files/fius-report-04-sk1.pdf., 16 and 18.
[16] SWD (2017)275, 2, supra note 8.
[17] Council 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.
[18] 'IBA Anti-Money Laundering Forum – Europe', accessed January 9, 2019, https://www.anti-moneylaundering.org/Europe.aspx.
[19] Directive 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.

Directives[20], which were adopted in 2001 and in 2006 respectively. The Second AML Directive established a broader definition of ML and included underlying offences within its scope.[21]

Five years later, the Third AML Directive introduced the risk-based-approach[22], which required businesses falling within its scope to carry out a risk-assessment of their customers, based on a variety of factors.[23] In accordance to the risk attributed to a particular customer, the obliged entity had to apply Customer Due Diligence (CDD) measures along the 'Know Your Customer' concept.[24]

In May 2015, the Fourth AML Directive was adopted, further regulating the processing of personal data by FIUs[25] and increasing their capacity to cooperate.[26] For instance, the Directive seeks to ensure timely and unrestricted access by FIUs to relevant financial data[27], to empower FIUs to take urgent action[28] and to improve coordination and cooperation between FIUs.[29] In addition, the Directive requires obliged entities to provide FIUs with *all necessary information*[30] and to hold a central register on their beneficial ownership to which FIUs and other competent authorities shall have access.[31] Moreover, the Directive suggests that FIUs should *exchange information freely, spontaneously or upon request*, with third-country entities.[32]

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, amendments to the Directive (Fifth AML Directive[33]), thereby expediting the transposition date of the latter by five months.[34] Initially, the proposal suggested that FIUs should be able to request information from obliged

[20] Directive 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.
[21] 'IBA Anti-Money Laundering Forum – Europe'.
[22] Special 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.
[23] For 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: Bergström, 1160, supra note 19.
[24] Ibid.
[25] Commission 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.
[26] SWD (2017)275, 2, supra note 8.
[27] Article 30(2) of Directive (EU) 2015/849.
[28] Article 32 (7) of Directive (EU) 2015/849.
[29] Recital (54) of Directive (EU) 2015/849.
[30] Article 33(1)(b) of Directive (EU) 2015/849
[31] Article 30(6) of Directive (EU) 2015/849.
[32] Recital (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.
[33] Proposal 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.
[34] To 1 January 2017, Patricia Taylor, 'The Fourth EU Anti-Money Laundering Directive – Impact on Investment Funds', 7 October 2016, https://www.williamfry.com/newsandinsights/news-article/2016/10/07/the-fourth-eu-anti-money-laundering-directive-impact-on-investment-funds.

entities without the need for a prior STR.[35] This, however, was changed in the final text along the European Data Protection Supervisor's (EDPS) Opinion[36] on the proposal.[37]

The Fifth AML Directive[38] reinforces the framework for the assessment of high-risk third-countries, addresses risks related to anonymous prepaid cards and virtual currencies and contains rules on cooperation between AML and prudential supervisors.[39] Moreover, the Directive seeks to strengthen the current requirements concerning cooperation between national authorities and to improve cross-border cooperation.[40] The amendments reinforce the preventive framework against ML, in particular by addressing emerging risks and by broadening the capacity of competent authorities to access and exchange information.[41] On 19 June 2018, the Fifth AML Directive was published in the Official Journal of the EU and must be transposed by 10 January 2020.[42]

On 11 October 2018, a Directive on countering ML by criminal law[43] was adopted, complementing the Fifth AML Directive.[44] The Directive establishes minimum rules on the definition of criminal offences and sanctions in the area of ML, requiring Member States to implement national laws providing for ML offences by individuals to be punishable by a maximum term of imprisonment of at least four years.[45] The Directive is based on Article 83(1) TFEU and thus, seeks to improve judicial cooperation in criminal matters and to reinforce the application of the Fifth AML Directive by tackling ML by means of criminal law.[46]

In April 2018, the Commission proposed a Directive laying down rules and measures to facilitate access by competent authorities to financial and bank account information for the prevention, detection, investigation or prosecution of serious criminal offences.[47] The proposal seeks to extend the exchange of (financial) information to the broader scope of serious crime. Besides enhanced procedures for LEAs to obtain information from obliged entities, the proposed Directive also provides for measures to facilitate access by FIUs to LE-information.[48] Being based on Article 87(2) TFEU, the proposal seeks to facilitate cooperation between FIUs in the different Member States by, *inter alia,* setting time limits

[35] Recital 14 of the proposed Fifth AML Directive.
[36] EDPS, 'EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications', Opinion 1/2017, 2 February 2017.
[37] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180417_directive-proposal-facilitating-use-information-prevention-detection-investigation-prosecution-criminal-offences_en.pdf.
[38] 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.
[39] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the Economic and Social Committee and the Committee of the Regions on Strengthening the Union framework for prudential and anti-money laundering supervision for financial institutions, Brussels, 12 September 2018, COM(2018) 645 final, 2.
[40] Ibid, 7. See also recital 16 of the amendments to the Fourth AML Directive.
[41] Cf.: 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).
[42] European Commission, 'Anti-money laundering and counter terrorist financing' https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en. Accessed on 07 January 2019.
[43] Proposal 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.
[44] '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/.
[45] 'EU Agrees Countering Money Laundering By Criminal Law Directive - Government, Public Sector - European Union', accessed January 9, 2019, http://www.mondaq.com/uk/x/712570/Money+Laundering/EU+Agrees+Countering+Money+Laundering+by+Criminal+Law+Directive.
[46] COM(2016) 826 final, recital 1, supra note 43.
[47] As defined in Annex I of Regulation (EU) 2016/794. See: COM(2018) 213 final, supra note.
[48] Article 1(1) of COM(2018) 213 final, supra note 2.

for replying to requests for information.[49] In accordance with Article 5(1) of the proposed Directive, access shall take place on a case-by-case basis and only be granted to designated persons within a competent authority. However, under Article 4(1), the latter authorities shall have the power to search bank account information *directly and immediately* for the performance of their tasks, without the need for prior judicial authorization.[50] The designated competent authorities are not defined in the proposal[51], nor does the latter specify the procedures for international transfers.[52] In addition, data subject rights are not mentioned in the proposed Directive, which solely refers to measures that shall be adopted to restrict *in whole or in part, the data subject's rights of access*.[53] These provisions are unlikely to be in compliance with data protection standards[54] and would be in violation of relevant jurisprudence of the Court of Justice of the European Union.[55]

All three instruments mentioned above seek to contribute to the fight against ML and TF by establishing rules on better access to financial information and by facilitating the exchange of such information between different bodies.[56] However, while the Fifth AML Directive is based on Article 114 TFEU, on the approximation of laws in the internal market, and solely addresses *preventive* efforts against ML and TF, both the proposed Directive on measures to facilitate LE-access to financial information and the Directive on countering ML by criminal law find their legal bases under Title V of the TFEU. Using Article 87(2) and Article 83(1) respectively reinforces the legal framework with regard to police and judicial cooperation.[57] It could, therefore, be argued that the wider regulatory AML framework shifted away from a predominantly single market focus to including organized crime more generally within an internal security context.[58] This also implies consequences regarding the way in which personal data may be collected and exchanged.

II.1. *Obstacles to the cooperation between Financial Intelligence Units*

As mentioned above, FIUs are operationally independent and autonomous entities that analyse, request and disseminate financial information. Such independence means that they receive STRs directly from the reporting entities, (generally) without interposition of third parties.[59] An FIU may be established as part of an existing authority, its core functions should, however, be distinct from those of the principal authority.[60] However, in some cases, obliged entities are required to simultaneously forward the same information to other domestic (LE) authorities, thereby blurring the distinction between financial analysis and investigation.[61]

[49] Article 9 of the proposed Directive, see COM(2018) 213 final, 12, supra note. 2.
[50] This was emphasised by the Regulatory Scrutiny Board as one of the main considerations concerning the proposal. See: Regulatory Scrutiny Board Opinion, 'Proposal 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', Strasbourg, 17 April 2018, SEC(2018) 197, 3.
[51] EDPS, 'Formal comments of the EDPS on the Proposal for a Directive of the European Parliament and of the Council on facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences', 10 September 2018, 3. ('EDPS comments of September 2018').
[52] Recital 27 solely refers to the provisions for international transfers under the LED and the GDPR.
[53] Article 15 COM(2018) 213 final, supra note 2.
[54] Both the European Commission Regulatory Scrutiny Board and the EDPS emphasized that there is a need for a strong justification to broaden access and the necessary safeguards have to be provided, see: European Commission Regulatory Scrutiny Board, 'Impact Assessment / Broadening access to centralised bank account registers and enhancing cooperation between FIUs and LEAs, Ares(2018), 31 January 2018 and COM(2018) 213 final, 7, supra note 2. Also see EDPS comments of September 2018, supra note 53.
[55] See, for instance, the Court's case law on data retention and access to stored data in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (C-293/12) and *Seitlinger* (C-594/12), ECLI:EU:C:2014:238, 8 April 2014, or Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* (C-203/15) and *Watson* (C-698/15), ECLI:EU:C:2016:970, 21 December 2016.
[56] EPRS, '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.
[57] Ibid, 3.
[58] Bergström, 1164, supra note 19.
[59] SWD(2017) 275 final, 4, supra note 8.
[60] FATF Recommendations, 'International standards on combating money laundering and the financing of terrorism & proliferation', 97.
[61] SWD(2017) 275 final, 5, supra note 8.

During the process of information gathering, FIUs may request information from their counterparts[62] in other Member States.[63] 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 FIUs' functions, tasks, independence and domestic statuses.[64] These different models may be separated into *administrative FIUs*, *law enforcement FIUs* and *mixed* or *hybrid FIUs*.[65] Although FIUs should exchange information with foreign FIUs regardless of their respective model[66], obstacles regarding the access to, exchange and use of information and the operational cooperation exist due to the different national structures.

In data protection law, different rules apply when processing is carried out for administrative or LE-purposes. Thus, their respective model has an impact on the way in which FIUs may process and exchange information and the type of analysis that they are authorized to carry out. Whereas administrative FIUs must process personal data under the GDPR's data protection regime that applies to all processing activities that pursue administrative purposes, FIUs that are considered LE-FIUs may process personal data within the scope of the LED, which applies where data are processed for the prevention, investigation, detection, or prosecution of crime.[67] Consequently, not all FIUs have access to the same information sources, as some might have limited access, for instance, to LE-information.

Following from the fact that FIUs are organized in different ways and have different domestic powers in accessing, sharing and using information, FIUs encounter problems when exchanging data received from obliged entities and LEAs.[68] While LE-FIUs normally have LE-powers, including the power to freeze transactions and seize assets[69], administrative FIUs may be far more restricted when processing personal data for their analyses. This leads to an information gap between different types of FIUs[70], since LE-FIUs, on average, have better access to national police and judicial data[71] and may face limitations when cooperating with administrative FIUs in cross-border investigations.[72]

In 2016, the computer network FIU.net[73] was incorporated into Europol to enhance the exchange of financial intelligence and to make Europol information hub within FIU.net,[74] another indication for the

[62] In the EU, in October 2000, Council Decision 2000/642/JHA was adopted concerning arrangements for cooperation between FIUs of the Member States with respect to exchanging information. This resulted in the FIU.NET initiative in 2002, which was promoted as decentralized and sophisticated computer network supporting the EU FIUs in their goal of information sharing.

[63] https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net. A request for international cooperation is sent when access to further information at national level is deemed insufficient to determine whether the reported transactions are relevant. Personal data are usually only shared if there is a hit See: Amicelle/Chaudieu, 651 and 658.

[64] SWD(2017) 275 final, 4, supra note 8.

[65] PE 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 FIU, 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.

[66] FATF Recommendations, 'International standards on combating money laundering and the financing of terrorism & proliferation' (2012-2018) 107.

[67] This means that whenever LE-FIUs process data for administrative purposes, they have to apply the general legal data protection framework.

[68] SWD(2017) 275 final, 4, supra note 8.

[69] In 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.

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

[71] Project '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.

[72] SWD(2017) 275 final, 5, supra note 8.

[73] FIU. NET is, via Europol, also connected to other channels and open source tools such as *World-Check*, which is part of Thomson and Reuters. *World-Check* compiles a master sanction list, counter-terrorism watchlists and other law enforcement databases that may be matched against the FIU.NET datasets. See: Amicelle/Chaudieu, 659, supra note 29.

[74] 'Financial Intelligence Units – FIU.net', Europol, accessed January 11, 2019, https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net.

increased involvement of LEAs, which has been criticised by some FIUs that fear extensive police engagement.[75]

This involvement of competent national authorities that are responsible for prosecution could impair the independence of FIUs when carrying out their investigations. The requirement for some obliged entities to forward their STRs to LEAs could diminish the delineation between the analytical tasks of FIUs and the prosecuting tasks of LEAs. Such blurring of tasks between supposedly financial analysis and investigation is reinforced by the recent Commission proposals to grant more LE-access to financial information.

Interim Conclusion

On the one hand, the choice to deliberately establish separate entities for the receipt and analysis of financial information and those to engage in investigations against AML and CTF, is criticised as creating an institutional gap between FIUs and LEAs.[76] A further merging between FIUs and LEAs could, however, have a negative impact on the independence of FIU, in particular, where they are incorporated under the same organizational structure as the national LEAs. As a consequence, the role of FIUs as neutral intermediary could be diminished and fail to fulfil its purpose.[77] Moreover, if LEAs obtain more and more capacities to access personal (financial) data themselves, the need for such an intermediary would be brought into question.

On the other hand, because both FIUs and LEAs continue to be faced with obstacles in their interactions, inter alia due to the different existing models and the way in which FIUs are authorized to process and exchange information, this existing distinction into different types of FIUs might be misleading. Here, the question would be whether FIUs would not generally fall within the definition of a competent authority under the LED, as they are processing data for LE-purposes whether by collecting STRs or by being directly engaged in investigations. In order to preserve the role of FIUs in between the private sector and LEAs, it would be essential to further enhance the effectiveness of their work by having the Member States clarify their powers and cooperation between them. One way to establish more clarity regarding the way in which FIUs may process and exchange information could be the application of the new harmonized data protection rules under the LED. The new rules provide for enhanced data protection standards in a LE-context, while giving competent authorities more flexibility when carrying out processing activities.

## III. The EU Data Protection Reform: Different Standards under GDPR and LED

On 25 May 2018, the GDPR entered into application, thereby forming the major part of the EU Data Protection Reform. The GDPR is accompanied by the LED, which is applicable for processing of personal data in the LE-context and which had to be transposed into the national laws of the EU Member States by 6 May 2018. As mentioned above, the scope of the GDPR covers general processing activities by private and public bodies, while the LED only applies when processing is carried out by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offences. Thus, in order for the Directive to be applicable, both personal and material scope must be satisfied.

[75] Some FIU officials remain reluctant regarding the network arguing that the link between FIU.NET and Europol is not sufficiently clear. Moreover, issues regarding IT-security, and data processing activities have been expressed regularly. See: Amicelle/Chaudieu, 658, supra note 29.
[76] K. Stroligo, C.L. Hsu and T. Kouts, 8, supra note 15.
[77] It needs to be mentioned that in some Member States, FIUs have actually more access powers than LEAs and thus, may provide LEAs with information that the latter normally would not have access to. Nevertheless, the role of intermediary remains, as FIUs are specialized entities that might be more competent to judge on which tailored information to provide to LEAs.

The LED replaced a Framework Decision from 2008[78], which was applicable solely to cross-border processing of personal data between competent Member State authorities, while not covering the processing of personal data *within* the territory of the Member States. Being applicable to such domestic processing, the LED put forth great achievements in an area that had previously not been regulated by EU law.[79]

Data processed by LEAs within the scope of the LED must be collected for specified, explicit and legitimate purposes, and not be processed in a manner that is incompatible with those purposes.[80] In the LE-context, this means that processing is lawful if carried out for the purposes stipulated under Article 1(1) LED.[81] Moreover, processing must be adequate, relevant and not excessive in relation to the purpose for which the data are processed. Pursuant to Article 5 LED, Member States are to establish time limits for erasure, storage and periodic review of the need to store personal data.[82] Some of the new obligations for controllers will be mentioned in the following section.

Since the Directive is not a full harmonization instrument, its scope and application depend on the transposition within the individual Member States. Consequently, this may lead to divergences among the Member States where some include more competent authorities within the definition of the personal scope of the LED than others.

While some FIUs do not even analyse the data that they receive and only develop databases that are directly available to LEAs, other FIUs can actively be involved in investigations. Accordingly, where FIUs are considered competent authorities under the national laws transposing the LED, processing carried out by these LE-FIUs falls within the scope of the Directive whenever those FIUs process personal data for the purposes of preventing and combatting financial crimes. However, it needs to be noted that even LE-FIUs may only apply the LED where both its personal and material scope are satisfied. In accordance with Article 9 LED, where competent authorities process non-LE data, the GDPR applies to their processing.

When processing personal data within the scope of the LED, LE-FIUs will be less restricted to receive and exchange data from and with other competent authorities and to transfer those data to third countries. Moreover, the obligation to provide data subject rights of access or information are less stringent as granting those rights could jeopardize ongoing investigations.[83]

On the other hand, this means that the Directive provides lower standards regarding data subject rights than the GDPR. The same applies for the obligations imposed on controllers, since, in the field of LE, more flexibility when processing personal data is crucial. Consequently, transparency obligations towards data subjects are naturally less strict than under the GDPR's framework.

III.1. The LED as instrument to achieve better FIU cooperation?

The LED was to be transposed into the national laws of the Member States in May 2016. Being the first horizontally and legally binding instrument for national *and* cross-border processing of personal data in the LE-area, the LED constitutes a major step forward in establishing a comprehensive EU data

[78] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350/60.
[79] Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' (December 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3285873.
[80] Article 4(1)(b) of Directive (EU)2016/680.
[81] Thus, for the 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.
[82] EPRS, 'LE-access to financial data', PE 615.665 (April 2018) 4.
[83] In accordance with Article 13(2)(d), data subjects must be notified once notification can no longer jeopardize ongoing investigations.

protection regime.[84] The Directive improved the level of fundamental rights protection in the area of police and criminal justice, and unified the data protection rules for personal data sharing between the Member States.[85] Being applicable to all types of processing for LE-purposes[86] carried out by competent authorities, the LED introduced major changes, while leaving certain leeway to competent authorities when performing their processing tasks:

Other than the GDPR[87], Article 8 of the Directive only provides for one legal basis, namely if processing is necessary for the performance of a task carried out by a competent authority for the purposes of the LED and based on Union or Member State law. That Article, therefore, provides for more discretion regarding the purpose limitation principle.[88] At the same time, Article 6 LED introduced a specific obligation for controllers to establish a clear distinction between personal data of different categories of data subjects (suspects, convicts, victims, witnesses).[89]

Another notable difference between the LED and the GDPR is the principle of data minimisation. While under Article 5(1)(c) GDPR processing should be *adequate, relevant and limited to what is necessary*, Article 4(1)(c) of the Directive stipulates that personal data shall be *adequate, relevant and not excessive*. This principle grants more flexibility to LEAs in the performance of their tasks compared to the requirements of the corresponding provision under the GDPR.[90]

The approach towards data subject rights and their possible limitations is supposed to adapt the means of processing personal data to the needs of LEAs. The controller may limit the right to specific information to be given to the data subject, the right of access and the right to obtain information about the possible refusal of rectification, erasure or restriction of processing in a similar way as under Article 23 GDPR.[91] Articles 13 and 15 LED lay down the specific conditions under which the right to be informed and the right of access may be restricted, clarifying that a restriction has to be laid down in law, respect the essence of the fundamental rights and freedoms of the data subject and must constitute a necessary and proportionate measure in a democratic society.[92]

Another key achievement of the LED is the obligation under Article 25 to keep access logs that aim at helping to detect data protection or security breaches, such as unauthorized or unusual access to a system.[93] The obligation to keep logs of six processing operations (collection, alteration, consultation, disclosure including transfers, combination and erasure) in automated processing systems is a distinct feature of the Directive, without any equivalent provision in the GDPR.[94] Article 25 LED applies to all automated processing systems, which practically means that all LE-databases must be in compliance with the obligation to keep logs.[95]

As a general rule, international transfers under Articles 35 to 38 of the LED shall be allowed only from one LEA to another, subject to authorization by the originating Member State.[96] The Directive incorporated the three-step cascading system (adequacy decision - appropriate safeguards - derogations) that was adopted under Articles 45-49 of the GDPR for international transfers. However, the approach to data transfers by way of appropriate safeguards gives more flexibility to controllers. Under certain

[84] See: Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017) 324-340.
[85] Sajfert/Quintel, supra note 75.
[86] The LED does not apply to processing of personal data in the course of an activity, which falls outside the scope of Union law, e.g. processing for national security purposes.
[87] Article 6 of the GDPR provides for six different legal bases.
[88] Sajfert/Quintel, 6, supra note 75.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] EDPS comments of September 2018, 5, supra note 50.
[93] Ibid, 3.
[94] Sajfert/Quintel, 15, supra note 75.
[95] Ibid, 16.
[96] Although this is already the case for FIU cooperation: an FIU cannot disclose the [received] information outside its agency without the prior written permission of the disclosing FIU, Egmont Group of FIUs 'Charter' (2013) 22.

conditions, Article 39 LED provides for so-called *asymmetrical transfers* from a LEA in a Member State to private parties in a third-country.[97]

The above examples[98] demonstrate that the reformed data protection framework for police and criminal justice authorities provides for robust safeguards while granting sufficient flexibility to process personal data in the LE-context. Moreover, whenever the material scope of the LED is not satisfied, competent authorities must revert to the GDPR. Consequently, where LE-FIUs carry out processing of personal data for purely administrative purposes, such processing falls within the scope of the GDPR.

**Conclusion**

Against the need of FIUs to be able to cooperate more efficiently and the proposed rules to grant LE-access to financial (and other) information for the prevention, detection, investigation or prosecution of certain criminal offences, finding the right balance between effective AML and CTF measures and the protection of fundamental rights is imperative.

The adding of new purposes for processing and the broadening of LE-access to personal data may be observed in other areas of EU Law.[99] These developments blur the line between administrative and criminal law. That distinction, however, is essential for EU data protection law, as the purpose of the processing is decisive for determining the applicable data protection instrument.

Moreover, access to additional information for various purposes that are not linked to the initial purpose of processing risks impairing the purpose limitation principle enshrined in Article 8(2) of the EU Charter[100], one of the cornerstones of data protection law. While it is arguable in how far this principle may be complied with where FIUs and LEAs carry out intelligence-based analyses and automated cross-matching of data, their processing activities should nevertheless comply with the updated EU data protection *acquis*.

The new data protection rules under the LED might be a first step to establishing a more harmonized framework in which FIUs and LEAs can rely on the same rules when exchanging data. While it is true that those rules only apply to FIUs that are considered competent authorities within the meaning of Article 3(7) LED, the improved standards under the Directive could ensure an adequate level of protection when cooperation between FIUs and also LEAs takes place. Separating between the applicability of the GDPR and the LED in accordance with the current typology between different FIU models is misleading, as FIUs, by *preventing* criminal activity, would fall within the scope of the LED.[101]

---

[97] Sajfert/Quintel, 7, supra note 75.

[98] There are evidently additional provisions that demonstrate the strengthened data protection standards under the LED, for instance, the provisions on remedies, liabilities and penalties, the strengthened role of national supervisory authorities, or Article 11 on automated individual decision-making and profiling. However, due to limitation of space of this contribution, the above examples were chosen to demonstrate some of the most striking provisions of the LED.

[99] For instance, in the context of migration and asylum, more purposes have been added to EU databases and LE access has been widened for all IT systems, cf.: Teresa Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (March 1, 2018). University of Luxembourg Law Working Paper No. 002-2018. Available at SSRN: https://ssrn.com/abstract=3132506. or http://dx.doi.org/10.2139/ssrn.3132506. The e-evidence proposal from April 2018 suggests direct LE-access to data help by service providers, irrespective of their location, cf.: Mark D. Cole and Teresa Quintel, 'Transborder Access to e-Evidence by Law Enforcement Agencies' (May 11, 2018). University of Luxembourg Law Working Paper No. 2018-010. Available at SSRN: https://ssrn.com/abstract=3278780 or http://dx.doi.org/10.2139/ssrn.3278780.

[100] As well as under Article 5(1)(b) GDPR, Article 4(1)(b) LED, Article 4(1)(b) of Regulation (EU)2018/1725 regarding the processing of personal data by Union bodies and institutions, the Europol Regulation, or Council of Europe Convention 108+ under Article 5(1)(b).

[101] Several national legislators, in the exercise of transposing the LED, even interpret the Directive's Recital 12 in a way that opens the possibility to include minor offences within the scope of the Directive. In other Member States, all types of offences are considered criminal offences and thus, trigger the applicability of the Directive in a general manner. Most of the Member States, however, will apply the Directive solely to *classic* criminal offences; consequently, in those Member States the GDPR will be applicable to minor offences. See: Sajfert/Quintel, 4, supra note 75.

Allowing FIUs to gather, analyse and exchange data more flexibly might improve the effectiveness of their cooperation and could help maintaining their role as intermediary between the private sector and LEAs. FIUs could support each other in their financial analysis and serve as a 'buffer' towards broadened LE-access to personal data: Given the increased access capacities to personal data granted to national LEAs, it is necessary to have a certain intermediary 'filtering', which could be achieved through the analysis of FIUs. Yet, harmonized data protection rules will not solve the problem. In order to carry out their analyses effectively, FIUs will also need to obtain the needed capacities and resources. Moreover, domestic statuses and organizational structures, as well as the operational autonomy of FIUs should be aligned.