Cooperation Between Financial Intelligence Units in the EU: Stuck in the Middle Between the GDPR and the Police Data Protection Directive

Organised crime, corruption and fraud (to name a few) generate significant amounts of wealth. We are all familiar with the occasional movie scene, where a renowned drug dealer resorts to burying thousands upon thousands of banknotes in their yard – but, as useful as that may be for hiding the money, it is of little help when one wants to spend it. Criminals who accumulate wealth cannot safely enjoy the proceeds of their efforts unless they 'launder' it first. In other words, they need to disguise the illegal origin of their proceeds – or else, they will attract the attention of law enforcement. The good news for those who are trying to launder their money is that, in today's globalised world, money flows across borders with the touch of a button; they have plenty of opportunities to integrate their illicit proceeds into the financial system and successfully distance their funds from the underlying crime. For law enforcement officials, however, who are on the trail of 'dirty' money, this is anything but good news; money travels easily, but they don't. As such, the *raison d' etre* of anti-money laundering (AML) regimes around the world, largely modelled after the Recommendations of the Financial Action Task Force (FATF), is to make money movements visible and therefore enable law enforcement to trace them.

The EU entered the anti-money laundering race in 1991, with the adoption of a Directive 'on the prevention of the use of the financial system for the purpose of money laundering'.[1] More than two decades and five Directives later,[2] the EU's anti-money laundering regime has evolved significantly – always in line with the FATF Recommendations.[3] To make

---

1 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 L 166/77 (First AML Directive).

2 First AML Directive; Directive 2001/97/EC of the European Parliament and of the Council 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, [2001] OJ L 344/76 (Second AML Directive); Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the Prevention of the use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (Text with EEA relevance), [2005] OJ L 309/15 (Third AML Directive); 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 (Text with EEA relevance), [2015] OJ L 141/73 (Fourth AML Directive); Directive 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 (Fifth AML Directive).

3 Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Launderign Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 2 *Maastricht Journal of European and Comparative Law* 261.

money movements traceable, the regime introduced a series of preventive measures, largely based on the collection of information by the regulated sector. Perhaps the most drastic among them is the obligation to report suspicious transactions. This led to the emergence of an institutional machinery[4] that is responsible for administering the surveillance of money movements at the national level.[5] Partly because of the preventive nature of this regime and partly because the EU lacked competence in criminal matters at the time,[6] this was not assigned to the 'traditional' policing sector,[7] but special agencies were set up for this role.[8] These 'new policing' institutions became known as Financial Intelligence Units (FIUs).[9] Upon receipt of suspicious transaction reports, they analyse them and, if need be, disseminate the results of their analysis to law enforcement authorities or their counterparts in the EU and beyond. They are, in other words, the EU's financial intelligence hubs - nestled between the reporting and law enforcement sectors.[10] And, just as their partners from the reporting sector, they handle massive amounts of personal data every day.

The operation of FIUs has brought about many a challenges for data protection. This article, however, focuses solely on those raised by the exchange of information between them. After all, a large part of their day to day activities rests on the transnational arena. Why? Because reporting suspicious transactions would bring about scarce results in a world where money flows easily across borders, but information about money flows doesn't. This article begins by setting out the legal framework that governs FIU cooperation in the EU. It then moves on to examine the present-day uncertainty over the data protection framework that governs their

---

4 Ben Bowling and James Sheptycki, *Global Policing* (Sage, 2012) 69-70.

5 Anthony Amicelle and Gilles Favarel-Garrigues, 'Financial Surveillance: Who Cares?' (2012) 5 *Journal of Cultural Economy* 105. Terence Halliday, Michael Levi, and Peter Reuter, 'Global Surveillance of Dirty Money', (Center on Law and Globalization, 2014), http://orca.cf.ac.uk/88168/1/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf accessed 19 June 2020.

6 Commission, 'First Commission's report on the implementation of the Money Laundering Directive (91/308/EEC) to be submitted to the European Parliament and to the Council' COM (95) 54 final, 13-14, 16 - 17.

7 Michael Levi and Mike Maguire, 'Something Old, Something New; Something Not Entirely Blue: Uneven and Shifting Modes of Crime Control', in Tim Newburn and Jill Peay (eds.), *Policing: Politics, Culture and Control* (Oxford: Hart Publishing 2012).

8 John AE Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?', in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds.), *Reloading Data Protection* (Springer 2013).

9 Valsamis Mitsilegas, 'New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights: Part 1' (1999) 3 *Journal of Money Laundering Control* 147.

10 Marieke de Goede, 'The Chain of Security' (2017) *Review of International Studies,* 1-19.

(co)operation, and namely whether this subject to the General Data Protection Regulation, or to its law enforcement counterpart, the Police Data Protection Directive. The remaining of the article focuses on the 'FIU.net' – the decentralised network for information exchanges between EU FIUs – and on the data protection challenges that emerged from its recent integration into Europol.

Ultimately, what this article seeks to illustrate is that data protection has always been an afterthought in the context of FIU cooperation. Operational needs have always preceded and surpassed data protection considerations, resulting in a framework that poses significant challenges for the protection of personal data.

Data Transfers Between Financial Intelligence Units in the EU

The Evolution of the Legal Framework on FIU Cooperation

When the First AML Directive was adopted, criminal matters were beyond the scope of Community competence, so the EU legislator refrained from prescribing any details about the 'authorities responsible for combatting money laundering'[11] (as FIUs were described at the time) and there was no mention of their cooperation. The FATF Recommendations were also silent on the matter. Be that as it may, the initial indifference of the FATF towards FIUs did not last for long; it eventually broke its silence over FIUs when it updated its Recommendations in 2003[12] and has been engaged with them ever-since.[13] Needless to say, the EU legislator followed suit. Article 21 of the Third AML Directive mirrored the FATF Recommendation almost to the letter; Member States should establish an FIU 'responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation.'[14] That said, the Third Directive hardly dealt with the issue of FIU cooperation – with the exception of article 38, which placed the Commission under a duty to facilitate the coordination efforts of FIUs.[15] This light-touch approach was

11 Article 6, First AML Directive.

12 FATF, 'The Forty Recommendations' (2003), Recommendations 13, 26, 31 and Interpretative Note to Recommendation 26.

13 FATF, Recommendation 26 (2003).

14 Article 21(2), Third AML Directive.

15 Article 38, Third AML Directive.

similar to the FATF's at the time: Recommendation 31 merely called upon countries to ensure that their FIUs have effective mechanisms of cooperation in place.[16]

In the absence of detailed EU - or international – rules on FIUs for the better part of the regime's first decade, the Member States enjoyed ample discretion in choosing the model and powers of their respective FIUs.[17] As a result, when one looks at FIUs in the EU, a picture of diversity emerges; a series of administrative, police, judicial and 'hybrid' authorities, all sharing a common mandate, make up the EU's financial intelligence infrastructure. Most FIUs (twenty-one in total) have been established under an administrative or police model.[18] Five (those of Cyprus, Denmark, Greece, Hungary and the Netherlands)[19] blend characteristics from multiple models and so are classified as hybrid, whereas only one (Luxembourg) belongs to the judicial-type category.[20] Yet, this diversity initially created significant difficulties for the exchange of information between them.[21] In the course of the '90s, administrative FIUs could not share data with law enforcement or judicial FIUs - and vice versa.[22]

This problem was not unique to the EU, so it wasn't long before FIUs took the matter into their hands. The first coordinated attempt to overcome these obstacles took place in 1995, while the anti-money laundering regime was still at its infancy. In the summer of that year, a number of FIUs from around the world came together at the Egmont-Arenberg Palace in Brussels and formed what became known as the Egmont Group - a transgovernmental network of FIUs, whose priority was to stimulate cross-border cooperation between FIUs.[23] Over the past twenty-five years this network (who currently counts 164 FIU members) developed numerous standards aiming to facilitate the exchange of information between FIUs worldwide.[24] I mention this

---

16 FATF, Recommendation 31 (2003).

17 COM (95) 54 final (n 6).

18 The FIUs of Belgium, Bulgaria, Croatia, Czech Republic, France, Italy, Latvia, Malta, Poland, Romania, Slovenia and Spain are classified as administrative. The FIUs of Austria, Estonia, Finland, Germany, Ireland, Lithuania, Portugal, Slovak Republic and Sweden are classified as belonging to the police/law enforcement type. See EU FIUs Platform, 'Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information' (2016), 5 -7.

19 ibid., 7.

20 ibid.

21 Commission, 'Second Commission Report to the European Parliament and the Council on the Implementation of the Anti-Money Laundering Directive' (1.7.1998) COM (1998) 401 final, 14 – 15.

22 ibid., Annex 7.

23 Egmont Group, 'Statement of Purpose' (June 1997).

24 Egmont Group, 'Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases' (June 2001); 'Best Practices for the Exchange of Information Between Financial Intelligence Units' (2004); 'Operational Guidance for FIU Activities and the Exchange of Information' (July 2013); 'Egmont Group of Financial Intelligence Units Support and Compliance Process' (June 2014); 'Egmont Group of Financial Intelligence Units Charter' (July 2013).

development, because the Egmont Group's standards have influenced the Union's legal framework on FIUs to a significant degree (and continue to do so), much like the FATF has influenced the EU's anti money laundering regime as a whole.

By the time the Egmont Group was established, it had become apparent that only an EU-wide legal framework on FIU cooperation could address the obstacles to information sharing. Provisions on cross-border cooperation between FIUs, however, could not be incorporated into the existing AML Directive; this was a 'first pillar' measure and the EU could not regulate FIUs via the 'first pillar', because their conduct was viewed as a penal matter.[25] The solution came about in 2000, in the form a 'third pillar' Council Decision on FIU cooperation.[26] The latter, which covered information exchanges *solely* for the purposes of anti-money laundering and not counter-terrorist financing, called for FIU cooperation *regardless* of the differences in their institutional model.[27] As the Commission observed, this Decision was designed to reflect the principles developed by the Egmont Group.[28] Despite its reduced scope, this Council Decision (which was recently repealed)[29] governed the cooperation between EU FIUs for two decades. It also provided the incentive[30] for the creation of the FIU.net, a decentralised computer network that enables the exchange of information between FIUs in the EU up to this day.[31]

Even after the adoption of the Council Decision, information exchanges between FIUs in the EU continued to suffer from numerous shortcomings.[32] Advocate General Bot aptly summarised those in the *Jyske Bank Gibraltar* case. As he observed, while the intention of the Council Decision was to harmonise FIU cooperation in the Union, the rules nonetheless

---

25 COM (95) 54 final (n 6).

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

27 Article 3, Council Decision 2000/642/JHA.

28 Commission, 'Report on the implementation of the Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)' COM (2007) 827 final.

29 Commission, '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.

30 Council of the EU, Document 12831/01 (Presse 364, 16.10.2001), para. 14. See also Council of the EU, 'Information on the FIU.NET Project', Document 9459/02 (31.05.2002); Article 7 of Council Decision 2000/642/JHA.

31 For more information on the FIU.net, see Europol, 'Financial Intelligence Units – FIU.net' <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net> accessed 19 June 2020.

32 Commission, 'Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing' COM (2012) 168 final, 11.

remained '*minimal* in nature' and allowed Member States 'a significant degree of discretion as regards the extent of their cooperation'.[33] In response to the repeated calls at the EU level to strengthen FIU cooperation[34] and propelled by the FATF's reviewed Recommendations of 2012 which expanded the FIU-related provision significantly,[35] the Fourth Directive was the first in the long line of anti-money laundering Directives to deal with FIU cooperation in detail.[36]

A few months later, however, FIU cooperation came once more at the forefront of the legislative agendas – where it was to stay for years to come. The circumstances that led up to this development are particularly sad. In 2016, a series of terrorist attacks sent shockwaves through the Union. Inevitably, these events resuscitated EU policymakers' interest in counter-terrorist financing. So, it wasn't long before the Council called on the Commission to present proposals to 'strengthen, harmonise and improve the powers of, and the cooperation between Financial Intelligence Units (FIU's), notably through the proper embedment of the FIU.net network for information exchange in Europol (….)'. The Council wasn't alone; the Commission made similar calls, both through the European Agenda on a Security and the Action Plan against terrorist financing.[37] In light of this, it should not come as a surprise that the Commission tabled a proposal to amend the Fourth AML Directive in 2016.[38] And so there were Five.

But the evolution of the Union's legal framework on FIU cooperation didn't stop there. It seems that, after all those years of inactivity, the EU legislator's decision to deal with this

---

[33] Case C-212/11, *Jyske Bank Gibraltar Ltd* v. *Administración del Estado*, Judgment of the Court of Justice (Third Chamber) [2013] ECLI:EU:C:2013:270, Opinion of AG Bot, paras 63-70 (emphasis added). Thomas Incalza, 'National Anti-Money Laundering Legislation in a Unified Europe : Jyske' (2014) 51 *Common Market Law Reveiw* 1829.

[34] European Council, 'The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens' [2010] OJ C 115/1, 23; European Parliament, 'Report on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report)' (26.9.2013), A7-0307/2013, paras 99 – 100; Commission, 'Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds' SWD (2013) 21, 101 – 102.

[35] FATF Recommendations, 'Interpretive Note to Recommendation 29 (Financial Intelligence Units)' (2012).

[36] See also Foivi Mouzakiti 'Cooperation between Financial Intelligence Units in the EU: Challenges for the rights to privacy and data protection' in Katie Benson, Colin King, and Clive Walker (eds.), *Assets, Crimes and the State: Innovation in 21st Century Responses* (Routledge 2020).

[37] Commission, 'The European Agenda on Security' COM (2015) 185 final, 10, 13-14 and 17; 'Action Plan for Strengthening the Fight Against Terrorist Financing' COM (2016) 50 final, 7, 9.

[38] Commission, '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.

complex issue opened up a can of worms; cooperation between FIUs in the EU always seems to fall short in the eyes of policymakers.[39] In fact, while these developments were unfolding, the EU FIUs Platform was conducting a study of the obstacles to FIUs' access to and exchange of information.[40] In response to this study, the Commission published in 2018 a proposal for a Directive which aimed, among other things, to facilitate FIU cooperation.[41]

This Directive, which lays down rules 'facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences' was adopted in June 2019 and it repealed the above-mentioned 2000 Council Decision on FIU cooperation.[42] What is more interesting, however, is that the Directive was adopted in under the legal basis provided for by Article 87(2) of the Treaty on the Functioning of the European Union, which enables the EU to put forward measures regarding the collection, storage and exchange of information and common investigative techniques in relation to the detection of serious forms of organised crime, with the aim of establishing police cooperation between the Member States' competent authorities in relation to the prevention, detection and investigation of criminal offences. The Commission considers this legal basis to be appropriate, despite the fact that not all Member States have given police status to their FIUs.[43] What is more interesting, however, is that the Preamble of the Directive calls on the Commission to assess 'in the near future' whether the establishment of a coordination mechanism, such as an 'EU FIU' would be an appropriate measure to strengthen the cooperation of EU FIUs.[44] The latest Action Plan 'for a comprehensive Union policy on preventing money laundering and terrorist financing' indeed considers the establishment of such a mechanism and indicates that the Commission will table a proposal to that end in 2021.[45] With that in mind, let us take a closer look at the current legal framework on the cooperation between EU FIUs.

---

[39] Commission, 'On improving Cooperation between EU Financial Intelligence Units', SWD (2017) 275 final.

[40] EU FIUs Platform (n 18).

[41] COM (2018) 213 final (n 29).

[42] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, [2019] OJ L 186/122 (hereafter Directive 2019/1153).

[43] Commission, 'Impact Assessment accompanying the Proposal for a 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' SWD (2018) 115 final, 24.

[44] Preamble, para 22, Directive 2019/1153.

[45] Commission, 'Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' C (2020) 2800 final, 10 – 12.

The current legal framework on FIU cooperation

The Fourth AML Directive calls on Member States to ensure that 'FIUs cooperate with each other *to the greatest extent possible*, regardless of their organisational status'.[46] In particular, they must 'exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing (…)'.[47] Importantly, this Article gives effect to the data protection principle of purpose limitation in the specific context of FIU cooperation, and it does so in a twofold manner.[48] First, personal data between EU FIUs must be exchanged only if the purpose of the exchange is the *analysis* of that information by the recipient FIU. This means that the data cannot be used in support of an investigation or prosecution – unless, as we will see, the recipient FIU obtains the prior consent of its counterpart. Maintaining this distinction sounds simple enough – but alas, there is a fly in the ointment; some EU FIUs tend to blur the lines between analysis and investigation – a blurring which clearly undermines the principle of purpose limitation.[49] Second, personal data is to be exchanged only if the analysis focuses on possible *money laundering* or *terrorist financing* cases – and no other criminality. In practice this means that, when filing a request, the FIU must demonstrate that it needs this information to pursue a potential money laundering or terrorist financing case. This requirement, however, was recently relaxed with the adoption of the Directive law enforcement access to financial information.[50] This Directive, which includes a limited number of provisions on FIU cooperation, calls on Member States to ensure 'that in exceptional and urgent cases, their FIUs are entitled to exchange financial information or financial analysis that may be relevant for the processing or analysis of information related to terrorism or organised crime associated with terrorism'.[51] We see, therefore, two further categories added here: terrorism and organized crime associated with terrorism.

Aside from the possibility of spontaneous dissemination described above (where FIUs enjoy a certain level of discretion) there is one instance where they are *obliged* to share information with their EU counterparts, even in the absence of a specific request. This is when they receive a suspicious transaction report that is relevant to another Member State. In this case, they must

---

46 Article 52, Fourth AML Directive (emphasis added).
47 Article 53(1), Fourth AML Directive, as amended by the Fifth AML Directive.
48 EU FIUs Platform (n 18), 140 – 143.
49 EU FIUs Platform (n 18), 8.
50 Directive 2019/1153.
51 Article 9, Directive 2019/1153.

promptly share it with the FIU of that other Member State.[52] The justification behind this newly introduced requirement is that, at times, a suspicious transaction report may contain information that concerns a Member State other than the one that receives it. Let us take the companies that operate under the freedom to provide services as an example; these companies are established in one Member State but operate throughout the EU. But pursuant to the territorial principle that underpins reporting obligations, obliged entities must file a report to 'the FIU of the Member State in whose territory the obliged entity transmitting the information is established'.[53] This sometimes leads in a situation where the FIU of the Member State where the suspicious activity takes place does not receive the information, whereas the FIU that *does* receive it cannot do much about it, since it concerns events that occurred in a different Member State. Article 53(1) of the Directive seeks to rectify this loophole, although it is important to note that it represents a move towards a 'data sharing by default' attitude.

In line with the FATF and Egmont Group standards,[54] the Directive also provides that when responding to requests from their EU counterparts, FIUs may employ the *whole range* of the powers that are available to them domestically.[55] For instance, an FIU may contact a national bank to request an individual's financial records in order to respond to an EU counterpart's request. It doesn't have to be an obliged entity though; the FIU may consult one of the many domestic databases at its disposal. This means that the (very wide) range of powers that FIUs enjoy at the national level can now be activated for the benefit of their EU counterparts. More importantly, it also means that the pool of information that is available to EU FIUs has been expanded significantly. Operationally that might sound optimal, but this broadly framed obligation raises significant questions about the content of the requests. Article 53(1) of the Directive provides limited guidance in that regard: '[A] request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used'. Still, several issues remain unanswered. What constitutes sufficient justification in the context of a request? Should such requests be based on corroborated suspicion or should a lower threshold of suspicion suffice? Should the receiving FIU assess the validity of its counterparts' suspicion? What happens if a request is not sufficiently justified? These are valid questions – the answers to which entail significant consequences for the rights to privacy and data protection. Perhaps

---

52 Article 53(1), Fourth AML Directive.

53 Article 33(2), Fourth AML Directive.

54 EU FIUs Platform (n 18), 16.

55 Article 53(2), Fourth AML Directive (emphasis added).

unsurprisingly, the EU FIUs Platform[56] has suggested that assessing the validity of their counterparts' suspicion before FIUs activate their domestic powers on their behalf 'may go against the principle of "mutual recognition" of suspicions among EU FIUs'.[57] Indeed, a recent survey revealed that while some EU FIUs require 'adequately motivated requests' before they activate their domestic powers, they nonetheless do not second-guess their EU counterparts' suspicion.[58]

In all forms of FIU cooperation highlighted above, the EU legislator has ensured that the obstacles to information exchange are kept at a minimum. The instances where an EU FIU may refuse to cooperate with its EU counterpart also reflect this approach; according to Article 53(3) of the Directive, '[A]n FIU may refuse to exchange information only in exceptional circumstances where the exchange could be contrary to fundamental principles of its national law. Those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes'.

The EU legislator may be promoting a model of maximum information exchange between EU FIUs, but that does not mean that FIUs can use the information they receive from their counterparts as they wish. Above we saw that, pursuant to the principle of purpose limitation, FIUs must only use information in support of their tasks. This applies to exchanged information as well.[59] But that is not the only limitation. Firstly, Article 54 stipulates that the transmitting FIU may impose restrictions to the use of the exchanged information - restrictions which the receiving FIU is expected to comply with. Secondly, the Directive specifies that exchanged information must be 'used only for the purpose for which it was sought or provided' and that any further use or dissemination of the exchanged information to the national authorities is subject to prior consent by the providing FIU.[60] If the recipient FIU requests the consent of the transmitting FIU to share the exchanged information with, say, a prosecutor, the latter must give that consent as promptly and freely as possible.[61] In a provision that mirrors the Egmont

---

56 A network of EU FIUs established in 2006 which aims to facilitate, among other things, FIU cooperation. See Commission, Register of Commission Expert Groups <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3251> accessed 8 April 2020.

57 EU FIUs Platform (n 18), 170 – 171.

58 ibid.

59 Article 54, Fourth AML Directive.

60 Article 55(1), Fourth AML Directive.

61 Article 55(2), Fourth AML Directive, as amended by the Fifth AML Directive.

Group's standards almost to the letter,[62] the Directive provides that the only cases where an FIU may refuse to consent is when

a) the planned dissemination falls outside the scope of application of the AML/CTF provisions
b) it could impair an investigation and finally
c) it could violate the fundamental principles of national law of the Member State where the requested FIU is situated.[63]

Last but not least, the Fourth anti-money laundering Directive introduced a form of FIU cooperation that far exceeds information exchange. Pursuant to Article 51, the EU FIUs Platform shall assist FIUs with the *joint analysis* of cross-border cases. The Directive does not provide any guidance on what constitutes joint analysis or how it should be conducted, but its potential has not gone unobserved. On the contrary; FIUs have been working intensely, under the umbrella of the EU FIUs Platform, to develop 'new ways for FIUs to work together to have *a common output* at the end – with actionable outcome'.[64]

The FIU.net

In the previous section, we saw that pursuant to the anti-money laundering Directive, FIUs in the EU cooperate by:

a) spontaneously sharing, at their discretion, information or analysis that is of interest to another Member State to the FIU of that Member State
b) promptly forwarding the suspicious transaction reports that concern another Member to the FIU of that Member State and
c) replying to requests from their EU counterparts.

But how do they actually communicate with each other? Article 56 of the Directive calls on FIUs to use 'protected channels of communication'[65] and to that end, encourages them to rely on FIU.net, a decentralised computer network that 'shapes a virtual information cloud between the FIUs and their (over 550) distributed government, commercial and public information sources and it enables real time analysis of distributed dynamic information and knowledge

[62] Egmont Group of FIUs, 'Principles of Information Exchange Between Financial Intelligence Units' (July 2013), para 26.
[63] ibid.
[64] EU FIUs Platform, 'Minutes of the Meeting of the EU FIU Platform 10 June 2016', (30 July 2016) (emphasis added).
[65] Article 56 (1), Fourth AML Directive.

otherwise legally, organisationally, technically, and/or financially impossible to achieve'.[66]

Without getting into much technical detail, let us gain a better insight into the main features of FIU.net. Perhaps the most important feature of the network is its decentralised nature. What does this mean? It means that all EU FIUs have their own database, where they store suspicious transaction reports. To become a member of the FIU.net, each of those FIUs had to connect its internal database to FIU.net. This connection is achieved through an in-house (FIU.net) server. So, 27 EU FIUs participating in the network translates into 27 FIU.net servers – which explains why FIU.net is described as a *decentralized* mechanism for data exchange.[67] In other words, there is no central database and no centralized storage of data. Instead, all data connected to FIU.net is stored at an FIU.net database located in the premises of individual FIUs.[68] This structure guarantees that individual FIUs maintain control over their data (e.g. no other FIU can access it without their consent) but also a certain level of flexibility when it comes to their data governance practices. [69]

The most well-known feature of FIU.net, however, is the technology that comes with it – known as Ma3tch ('Match three'). This is an analysis tool, promoted as enabling 'FIUs to identify information that before would have remained undetected and there is no need to expose any privacy sensitive data'.[70] Ma3tch enables FIUs to (as its name suggests) *match* their data with the data of their EU counterparts, in order to determine whether they hold information that is of interest to them.[71] If there is a positive hit, the FIUs involved will be alerted and follow-up on the hit, by sharing the actual personal data.[72] As Balboni and Macenaite argue, this 'privacy by design' solution leads to improved privacy and data protection in the context of FIU cooperation, because it ensures that FIUs exchange only that data that is absolutely necessary – hence respecting the data protection principle of data minimisation.[73] By bringing the

---

[66] Udo Kroon, 'Ma3Tch: Privacy and Knowledge:'Dynamic Networked Collective Intelligence'' (2013) *2013 IEEE International Conference on Big Data* 23.

[67] ibid.

[68] ibid.

[69] ibid.

[70] See video on 'FIU.net and Ma3tch', https://vimeo.com/145121509, accessed 12 June 2020.

[71] Paolo Balboni and Milda Macenaite, 'Privacy by Design and Anonymisation Techniques in Action: Case Study of Ma3tch Technology' (2013) 29 *Computer Law and Security Review* 330.

[72] Anthony Amicelle and Killian Chaudieu, 'In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units' in Colin King, Clive Walker and Jimmy Gurule (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Cham:Springer International Publishing 2018), 658 - 659.

[73] Balboni and Macenaite (n 71).

information of FIUs together, Ma3tch enables EU FIUs to act 'as one' – at least in the virtual sphere.[74]

This account may have given the impression that FIU.net and Ma3tch are an integral part of all EU FIUs' daily routines. That, however, has not been the case;[75] - although the latest AML Directives are bound to change that. [76] To comply with the newly introduced forms of FIU cooperation that we explored above, FIUs will have to *routinely* participate in this virtual network. The requirements for joint analysis and cross-border dissemination of STRs are already occupying a series of pilot projects under the umbrella of the EU FIUs Platform.[77] Given that these new forms of cooperation – and especially the requirement to forward reports that concern another Member State to the FIU of that Member State -[78] impose a heavy workload on FIUs, they are keen to exploit the functionalities of FIU.net in order to comply with these obligations.[79] Despite their ongoing efforts to standardize cross-border dissemination of those reports via FIU.net, this functionality is not widely used yet.[80] The Commission, who in the summer of 2019 reviewed the status of FIU cooperation in the EU, concluded that 'few Member States today comply with their legal obligation to forward or disseminate cross-border reports'.[81]

But the far-reaching potential of Ma3tch does not end with cross border reports – or joint analysis.[82] FIUs can, for instance, use this technology to amalgamate their collective knowledge over risks or patterns of behaviour.[83] They can also use it for social network analysis, in order to identify relationships between entities.[84] All these possible additional uses of Ma3tch have not gone unnoticed by EU policymakers, who have big plans for FIU.net's future. In fact, the Commission recently noted that

---

74 Commission, 'FIU.net: empowering the FIUs and partners in their cross-border cooperation' https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2013_ISEC_FP_C1_4000005000_en> accessed 12 June 2020.

75 EU FIUs Platform, 'Minutes of the 33rd Meeting of the EU FIUs Platform' (12 December 2017), 8.

76 Article 56(2), Fourth AML Directive.

77 EU FIUs Platform, 'Minutes of the 42nd Meeting of the EU FIUs Platform' (11 December 2019).

78 Article 53(1), Fourth AML Directive.

79 EU FIUs Platform, 'Minutes of 30th Meeting of EU FIUs Platform' (16 December 2016).

80 Commission, 'Assessing the Framework for Cooperation Between Financial Intelligence Units' COM (2019) 371 final, 8.

81 ibid., 7.

82 Kroon (n 66), 27.

83 Erich Schweighofer, Vinzenz Heussler and Peter Kieseberg, 'Privacy by Design Data Exchange between CSIRTS', *Privacy Technologies and Policy* (Springer 2017), 104-119.

84 ibid.

> The FIU.net should be developed so that the system can be used to extract information and statistics on flows of information, activities and the outcomes of analysis. Having relevant, reliable, and comparable quantitative data at EU level will contribute to a better understanding of the risks and also help the Commission and the Member States to identify sectors that transmit few reports on suspected activities or transactions and analyse the reasons why.[85]

For most of its lifespan, FIU.net was administered by the Dutch Ministry of Interior,[86] with the support of a series of grands by the Commission.[87] In search for a long term solution, it was decided that FIU.net should be embedded in Europol and a Common Understanding was signed to that effect in 2013.[88] FIU.net was officially integrated in Europol three years later.[89] FIUs are connected to Europol through the Europol National Units.[90] This embedment, high in the list of political priorities,[91] was promoted as 'an opportunity for greater operational cooperation between FIUs and law enforcement'[92] that will benefit investigations into organised crime by increasing the 'synergies between financial and criminal intelligence'.[93]

Keen to examine how these synergies might translate into operational terms, in 2017 Europol launched a pilot project which involved the matching (via FIU.net and Ma3tch) of lists of high value targets within EMPACT priority areas[94] against the data of seven FIUs.[95] There

---

85 Commission, 'Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on 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', Annex 8.

86 European Parliament, Parliamentary Questions, Answer given by Mr Avramopoulos on behalf of the Commission, E-015304/2015 (February 2016).

87 Commission, Staff Working Document 'on the ex post evaluation of the "Prevention and fight against crime" 2007-2013 programme (ISEC) Accompanying the document Report from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ex post evaluation for the period 2007 to 2013 of the "Prevention and fight against crime" programme (ISEC) and the "Prevention, preparedness and consequence management of terrorism and other security related risks" programme (CIPS)' SWD(2018) 332 final, 31.

88 EU FIUs Platform, 'Minutes of 30th Meeting of EU FIUs Platform' (16 December 2016).

89 European Parliament, Parliamentary Questions (n 86).

90 EU FIUs Platform, 'Minutes of the 25th Meeting of the EU FIUs Platform' (28 September 2015).

91 Council of the EU, 'Outcome of the Council Meeting, 3432nd Council meeting, Justice and Home Affairs' (20 November 2015) Document 14382/15, 6.

92 Europol, Press Release of 5 September 2017 <https://www.europol.europa.eu/newsroom/news/global-anti-money-laundering-framework-—-europol-report-reveals-poor-success-rate-and-offers-ways-to-improve> accessed 19 Jun 2020.

93 Europol, 'Europol Programming Document 2018-2020' EDOC# 856927v18 (2018), 68.

94 EMPACT stands for European Multidisciplinary Platform Against Criminal Threats.

95 Europol, '2017 Consolidated Annual Activity Report' (3 May 2018), 43.

were high hopes for FIU.net's contribution in the 'fight' against terrorist financing as well;[96] according to official statements, the network was set to support the work of Europol's European Counter Terrorism Centre,[97] while FIUs would be able to request Europol to conduct searches at the Terrorist Finance Tracking Programme on their behalf.[98] A pilot was launched to that effect and in 2016 and 23 Member States gave the go ahead for their FIUs to have direct contact with Europol for this purpose.[99] These are just some of the pilot projects that were introduced following the embedment of FIU.net into Europol in order to explore possible data-driven synergies. As we will see in the following section however, all these aspirations came abruptly to an end, in the face of data protection considerations.

In this section, we examined the evolution of the Union's legal framework on FIU cooperation. We saw that, for the most part, FIU cooperation in the EU was governed by a patchy legal framework, which developed spasmodically largely in response to the FATF and Egmont Group's standards, and that it took a very long time until the EU legislator eventually decided to incorporate a series of substantive provisions on FIU cooperation within the fourth (and fifth) AML Directives. These provisions, which introduced several new forms of FIU cooperation, are supported by FIU.net and Ma3tch technology, although they are not exploited as much as EU policymakers would have liked. All this, however, comes at a cost – an invisible cost – for the protection of personal data, which has always been an afterthought throughout this evolution. In the following sections, we shall focus on that.

FIU Cooperation in the EU: Challenges for the Rights to Privacy and Data Protection

Uncertainty over the applicable data protection framework

[96] Council of the EU - EU Counter-Terrorism Coordinator, 'JHA agencies' role in counter-terrorism', Document 6146/18 ADD 1 (27 February 2018), 4. Commission, 'The European Agenda on Security' COM (2015) 185 final, 14.

[97] Council of the EU, 'Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing' Document 14244/15 (23 November 2015), 8.

[98] Europol, '2016 Consolidated Annual Activity Report', 32. See also EU FIUs Platform, 28th Meeting

[99] Council of the EU, 'Implementation of the counter-terrorism agenda set by the European Council', Document 13627/16 ADD 1 (4 November 2016), 26.

It would not be an overstatement if we claimed that 2018 was the year of data protection in the EU. In the spring of that year, the General Data Protection Regulation[100] (GDPR) became applicable and the deadline for the national transposition of its police and law enforcement counterpart – the Police Data Protection Directive[101] – expired. So, how does this recent reform affect FIU cooperation within the EU? Since FIUs were established, there has been a prevailing uncertainty over the data protection framework that governs their cross-border activities.[102] Unfortunately, the recent data protection reform did not bring about any clarity on that front – if anything, it has complicated matters.

Because FIUs in the EU are so diverse, it is not clear whether their domestic data processing activities are governed by the GDPR or by the Police Data Protection Directive. The answer to this question is not easy. To begin with, Article 41 of the Fourth anti-money laundering Directive states that Directive 95/46 (the GDPR's predecessor) applies to the processing of personal data for the purposes of that Directive.[103] It *also* states, however, that the Directive 'is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters'.[104] This caveat leaves us with no conclusive answer as to which data protection framework applies to FIUs. This has not gone unnoticed; when the European Data Protection Supervisor published his Opinion on the proposed Fourth anti-money laundering Directive, he suggested that '[i]n order to ensure seamless and effective data protection, and in view of the legal basis chosen for the Proposals, there should be no doubt that the activities of the competent authorities *and the FIUs* under the proposed Directive will *only* be subject to national provisions implementing Directive 95/46/EC'.[105]

The EU legislator, however, did not follow up on the EDPS' suggestion at the time – which might prompt us to conclude that the activities of FIUs were, in the EU legislator's view, subject

---

[100] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

[101] 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

[102] Mitsilegas and Vavoula (n 3).

[103] Recital 42 and Article 41, Fourth AML Directive.

[104] Recital 42, Fourth AML Directive.

[105] EDPS, 'Opinion of the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds' (4 July 2013), (emphasis added).

to the (now repealed) Framework Decision 2008/977 'on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters'.[106] There is, however, another plausible explanation for the EU legislator's reluctance to take a stance on this matter. Because FIUs come in different models, it is debatable whether the EU legislator can determine which data protection framework should apply to FIUs of a law enforcement, judicial, or even hybrid nature through a Directive that has been adopted under an internal market legal basis. The above-mentioned Framework Decision has now been repealed and replaced by the Police Data Protection Directive, but this doesn't affect our discussion. As the following analysis demonstrates, FIUs have struggled over this for some time.

In March of 2018, two months before the new data protection rules became applicable, the EU FIUs Platform raised the matter of the applicable data protection framework in a discussion that revealed the divergence of viewpoints between stakeholders.[107] For its part, the Commission emphasized that '*as a public administration*' FIUs fall under the GDPR.[108] But FIUs were not convinced; instead, they expressed concerns as to 'the applicability of the GDPR versus the directive in general and more specifically to administrative FIUs (…)'.[109] A few months later, the Platform revisited this issue.[110] The Commission noted that pursuant to Article 94 of the GDPR,[111] all references to the (repealed) Data Protection Directive within the anti-money laundering Directive are to be read as references to the GDPR. That means, the Commission continued, that Article 41 of the AML Directive, which provides that '[t]he processing of personal data under this Directive is subject to Directive 95/46/EC' is henceforth to be read that the processing is subject to the GDPR. Clearly, the Commission is of the view that Article 41 covers the processing of data by FIUs.[112] Some Member States, however, disagreed with this interpretation.

> One member reminded that according to AMLD 32(1) prevention and detection of criminal offences is a core responsibility of FIUs, furthermore they use on a very large scale police etc. data derived from criminal investigations. Another member referred to that several FIUs are

106 Mitsilegas and Vavoula (n 3).
107 EU FIUs Platform, 'Minutes of the 35th Meeting of the EU FIUs Platform' (8 June 2018).
108 ibid., (emphasis added).
109 ibid.
110 EU FIUs Platform, 'Minutes of the 37th Meeting of the EU FIUs Platform' (November 2018), 8.
111 Article 94 of the General Data Protection Regulation provides that 'Directive 95/46/EC is repealed with effect from 25 May 2018' and that 'References to the repealed Directive shall be construed as references to this Regulation'.
112 EU FIUs Platform, 'Minutes of the 37th Meeting of the EU FIUs Platform' (November 2018), 8.

> actually law enforcement authorities and that their core business are covered by the Data Protection Police Directive.[113]

But the Commission did not embrace the view that the processing of data by FIUs falls within the law enforcement sphere. In its opinion, the fact that some of them have law enforcement status is not enough for the Police Data Protection Directive to be applicable.[114] For the latter to apply, both the personal and material scope must be fulfilled – and even if an FIU satisfies the personal scope (ie if it qualifies as a 'competent authority' for the purposes of the Police Data Protection Directive), the Commission believes that carrying out analysis of suspicious transaction reports does *not* satisfy the material scope of the Directive – that is, the requirement that the data is processed for the purposes of *preventing, detecting or suppressing crime.*[115]

Clearly, this issue calls for some debate. Just as the European Data Protection Supervisor before it, the Commission seems determined to steer Member States towards applying the GDPR to their FIUs – but is this really the appropriate legal framework for them? First of all, not all of them qualify as 'public administration' – as the Commission described them. And second, even the FIUs that *do* qualify as administration might not necessarily fall under the GDPR's scope – and vice versa. For instance, the Greek FIU (which is a hybrid FIU)[116] applies the GDPR.[117] But the UK FIU *also* applies the GDPR – even through it is a law enforcement-type FIU.[118] Not all FIUs have opted for the GDPR though; Luxembourg's (judicial) FIU applies the Police Data Protection Directive.[119] This serves to illustrate that not all EU FIUs abide by the same data protection instrument. And when it comes to information exchanges between them, this complicates matters significantly.

It complicates them because the GDPR and the Police Data Protection Directive offer different degrees of protection when it comes to the processing of personal data. So when an EU FIU that applies the GDPR shares personal data with an EU counterpart that applies the Directive instead, the data in question is transferred to an environment that offers, at least to some extent, watered down protections compared to those offered where the data was collected in the first place. A detailed overview of the differences between the two legal instruments is

---

113 ibid.
114 ibid.
115 ibid.
116 The Greek FIU has strong law enforcement elements.
117 Interview with Greek FIU (November 2018).
118 Interview with UK FIU (August 2018).
119 Interview with Luxembourg FIU (January 2019).

beyond the scope of this article – but it is important that we highlight some of the differences that are relevant for the purposes of our analysis.[120]

With regards to data protection principles, the Directive does not require the processing of personal data to be transparent, whereas the GDPR does.[121] It also does not prohibit 'further processing' of data in the same way that the GDPR does: whereas the latter prohibits further processing of data for purposes other than those they were collected,[122] the Directive permits subsequent processing (by the same or another controller) if the controller is authorized do so and the processing is necessary and proportionate.[123] The Directive's take on the principle of data minimization also diverges from its 'first pillar' counterpart, so as to provide law enforcement authorities with more flexibility; according to the Directive, personal data must be 'adequate, relevant and *not excessive'*,[124] whereas under the GDPR, they must be 'adequate, relevant and *limited to what is necessary'*.[125] Principles aside, there are also important differences when it comes to the data subjects' rights. First of all, the Directive does not provide for a right to be forgotten or the right to data portability. Second, the rights to information,[126] access,[127] and rectification or erasure[128] are considerably limited under the Directive when compared to the GDPR. In particular, the Directive allows Member States to restrict them in order to a) avoid obstructing official or legal inquiries, investigations or procedures, b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, c) to protect public security, d) national security and e) the rights and freedoms of others.[129] Those rights can, of course, also be limited under the GDPR, but in the Directive's case there is understandably more room for limitations. For example, if a person is under investigation and files a subject access request with a law enforcement authority, they are likely to receive a 'nor confirm nor deny' type of response.

That said, we must also keep in mind that the Directive only provides a minimum level of harmonization; chances are, therefore, that additional divergences exist, depending on how

---

120 For a detailed overview of the differences between the GDPR and the Directive, see De Hert and Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) *New Journal of European Criminal Law* 7, 7-19.

121 Article 5(1)(a) of the GDPR and Article 4(1)(a) of the Police Data Protection Directive.

122 Article 5(1)(b), GDPR.

123 Article 4(2), Police Data Protection Directive.

124 Article 4(1)(c), Police Data Protection Directive.

125 Article 5 (1) (c), Police Data Protection Directive.

126 Article 13, Police Data Protection Directive.

127 Article 14, Police Data Protection Directive.

128 Article 16, Police Data Protection Directive.

129 Article 13(3), Article 15(1) and Article 16(4), Police Data Protection Directive.

Member States have chosen to implement it. All things considered, it seems clear that a Member State's choice to apply one or the other data protection instrument has real consequences for data subjects. And if we take into account that EU FIUs exchange large amounts of personal data on a routine basis, it is difficult to escape the conclusion that their cooperation continues to takes place – despite the recent data protection reform - under an uneven legal framework that undermines the protection of personal data.

To resolve this, I would argue that Member States should subject their FIUs to the *same* data protection framework – despite their institutional differences. This inevitably raises the question as to which is the most appropriate framework for FIUs – the GDPR or the Police Data Protection Directive. In the following section, I will argue that - in contrast to the Commission's view – Member States should subject their FIUs to the Police Data Protection Directive.

The Case for Subjecting FIUs to the Police Data Protection Directive

In order for the Directive to be applicable, two requirements must be met. The first is the material scope: the processing of personal data must take place 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.[130] But the presence of the material scope alone is not enough; for the Directive to apply, the processing in question must be carried out by *a competent authority* (personal scope). A competent authority is, according to the Directive,

> (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;
>
> b) or 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.[131]

The question before us therefore, is whether the processing of data by EU FIUs satisfies those two requirements.

---

[130] Article 2 (1) and Article 1(1), Police Data Protection Directive.

[131] Article 3 (7), Police Data Protection Directive.

Let us begin our analysis with the material scope - the prevention, investigation, detection and suppression of crime. The purpose of the FIU, according to the latest anti-money laundering Directive, 'is to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity *in order to prevent and combat money laundering and terrorist financing*, and to disseminate the results of its analysis as well as additional information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or financing of terrorism.'[132] In light of this, it is difficult to argue that the processing of data by FIUs does not satisfy the material scope of the Police Data Protection Directive.[133] For the Commission, however, this is not a clear-cut matter; as I mentioned earlier, in a recent meeting of the EU FIUs platform, its representatives argued that FIU analysis does not necessarily satisfy the material scope of preventing, detecting or supressing crime.[134] Given that the sole purpose of analysis is to identify connections between suspicious financial flows, money laundering and terrorist financing, I find the Commission's argument hard to sustain. Earlier Commission documents even contradict its current stance; the 2010 Communication on information management in the area of freedom, security and justice mentions the Council Framework Decision 2008/977/JHA (now replaced by the Police Data Protection Directive), the Council of Europe Convention 108 and the Council of Europe Police Recommendation R87 as the applicable data protection framework to FIU cooperation, including FIU.net.[135] Nonetheless, in its latest report on FIU cooperation, the Commission clearly stated that FIUs must abide by the GDPR's requirements.[136] At the same time, however, it acknowledged that '[d]espite this clear obligation, *most FIUs apply the Police Data Protection Directive* (…) instead or both the General Data Protection Regulation and the Police Data Protection Directive'.[137] Clearly, there is some controversy as to the appropriate framework for FIUs – and not all Member States see eye to eye with the Commission.

---

132 Recital 18, Fifth AML Directive (emphasis added).

133 See also Teresa Quintel, 'Follow the Money, if you can - Possible solutions for enhanced FIU cooperation under improved data protection rules' (University of Luxembourg, Law Working Paper Series, Paper number 2019-001).

134 EU FIUs Platform, 'Minutes of the 37th Meeting of the EU FIU's Platform' (11 November 2018).

135 Commission, 'Overview of information management in the area of freedom, security and justice' COM (2010)385 final, 14, 49.

136 Commission, 'Report from the Commission to the European Parliament and the Council – Assessing the Framework for Cooperation Between Financial Intelligence Units' (24/07/2019) COM (2019) 371 final, 12 (emphasis added).

137 ibid.

What complicates matters further, however, is whether FIUs satisfy the personal scope requirement; can we convincingly argue that *all* EU FIUs, irrespective of their status, satisfy the definition of competent authorities under the Directive?[138] In short, this is for the Member States to decide – and clearly the majority of them have decided that indeed they do. But their decision is not necessarily linked to the status of the FIU; the UK, for instance, decided to subject its FIU to the GDPR – despite the fact that the UK FIU is a police-type FIU, housed under the National Crime Agency. But a 2014 report about the UK's block opt-out of pre-Lisbon criminal law and policing measures, the European Scrutiny Committee examined (among other things) under which data protection framework the UK FIU would exchange information with its counterparts if they opted out of the Council Decision 2000/642/JHA (on FIU cooperation).[139] During this discussion, it was suggested that the UK FIU could perhaps continue to exchange information under a police-to-police framework – applying the so-called Swedish initiative[140] that governs information exchanges between law enforcement authorities. The government noted, however, that while the UK FIU would fit within the definition of a *law enforcement* authority, other FIUs would not.[141] Nonetheless, a few years later, the UK government decided that its FIU is more akin to administration and that the GDPR is the appropriate instrument to regulate its activities.

These inconsistencies serve to demonstrate that EU FIUs sit in the grey zone between administration and law enforcement. In other words, they sit in the zone between the former first and third pillar – and neither the Member States nor the EU legislator seem to be able to agree as to where their nature lies. But this ambivalence comes at the expense of legal certainty, because it is not clear which data protection framework governs their cooperation - at a time when, as we have seen, they become more and more interconnected. This dilemma raises a broader question: in cases where the lines between law enforcement and the administrative (or private) sector are blurred, how should the applicable data protection framework be determined? Should it be determined by reference to the nature of the data controller (are they a 'competent authority' or not?), or by reference to the (law enforcement) purpose of the data processing?

---

138 Article 3 (7), Police Data Protection Directive.

139 House of Commons, European Scrutiny Committee, *The UK's block opt-out of pre-Lisbon criminal law and policing measures: Government Response to the Committee's Twenty- first Report of Session 2013–14* (2013-2014 HC 978), 45 (emphasis added).

140 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89.

141 House of Commons (n 139).

Similar dilemmas have been raised when private entities are called upon to transfer data to public authorities for law enforcement and public security purposes – or to retain data so that the authorities can access them. In 2006, the CJEU dealt with the legal basis of the Council Decision on the Passenger Name Records Agreement between the EU and the US,[142] a post 9/11 measure which required airline companies to transfer passenger data to the US Bureau of Customs and Border Protection.[143] In this context, the Commission adopted a data protection adequacy decision under the (now repealed) Data Protection Directive. The CJEU held that the ('first-pillar') legal bases (current Art 114 TFEU and the Data Protection Directive) that those two decisions were adopted under were not appropriate, because the data processing operations related to matters of public security and law enforcement.[144] According to the CJEU, the transfers of data by private entities to public authorities for law enforcement purposes fell outside the scope of the (former) Data Protection Directive.[145] So, even though the data were initially collected in a commercial context and the data controller was a private entity, it was the *purpose* of the processing (public security and law enforcement) that determined the applicable data protection framework.[146]

But that criterion doesn't always prevail. Soon after the PNR judgement, the Data Retention Directive, a first-pillar measure that obliged electronic communication service providers to retain data 'in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime', [147] was challenged on the ground that it was not adopted under the appropriate legal basis.[148] In this instance, the CJEU did not follow the PNR judgment's logic. Instead, it held that the data retention obligations imposed by this Directive, even though they served crime-fighting purposes, were rightly based on the first pillar, because they covered the activities of service providers in the internal market.[149] The decision of the court in this instance has been criticised for creating an artificial distinction

---

142 Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [2004] OJ 2004 L 183.

143 Joint cases C-317/04 and C-318/04 Parliament v Council [2006] ECR I-04721.

144 ibid., 57.

145 ibid.

146 ibid.

147 Article 1(1), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105

148 Case C-301/06 *Ireland v Parliament and Council* [2009] ECR I- 00593.

149 Ibid., para 93.

between the storage of data for law enforcement purposes on the one hand, and the access and further processing of that data by the (law enforcement) authorities.[150]

To complicate matters further, in *Tele2/Sverige*, the court decided that national law which was based on Article 15(1) of the E-privacy Directive (which allows Member States to restrict some of the rights provided by the Directive for crime fighting purposes by, among other things, adopting data retention rules) and provided for the retention *and* access to data by public authorities for law enforcement purposes, fell within the scope of the E-privacy Directive.[151] In this instance the CJEU did not separate between retention and access

> 'since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services'.[152]

As Advocate General Saugmandsgaard Øe remarked in his Opinion on the so-called 'Schrems II' case, these two approaches are somehow conflicting.[153] This illustrates the dilemmas that arise when attempting to determine the data protection framework that governs transfers of data from 'first pillar' to 'third pillar' entities – or even beyond, in the realm of national security. The case of FIU cooperation is no exception, since, as we saw earlier, some FIUs are subject to the GDPR. If we take into account the PNR case, which mostly concerned data transfers, and considering that the recent Directive on law enforcement access to financial information, which includes (limited) provisions on FIU cooperation was adopted under Article 87(2) TFEU (which enables the Union to adopt measures on, among others, the exchange of information to facilitate police cooperation among Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences) I would argue that the more appropriate data protection framework to govern the exchange of information between FIUs is the Police Data Protection Directive – and not its internal market counterpart.

---

150 Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* (Springer 2012), 392 – 393.

151 Joined Cases C-203 & 698/15, *Tele2 Sverige AB* v. *Post-och telestyrelsen*, and *Secretary of State for the Home Department* v. *Tom Watson, Peter Brice and Geoffrey Lewis*, Judgment of the Court (Grand Chamber) of 21 December 2016, EU:C:2016:970, paras 67 – 81.

152 ibid., para 79.

153 Case C -311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems,* Opinion of AG Saugmandsgaard Øe [2019], para 213.

The Integration of FIU.net into Europol: Data Protection Challenges

The lack of clarity over the data protection framework that regulates information exchanges between EU FIUs is not the only issue that creates problems from a data protection perspective. In the previous section, I mentioned that despite the aspiring synergies between criminal and financial intelligence that would be developed by FIU.net's embedment into Europol, the curtain on that fell too soon. This happened in December of 2019, when the EDPS put an abrupt end to the embedment of FIU.net in Europol.[154] In order to understand why this happened, we need to take a closer look into the details of this arrangement. I will endeavour to do so without going into much technical detail.

In 2013, EU FIUs and Europol agreed upon a Common Understanding on the embedment of FIU.net into Europol.[155] As Europol noted at the time,

> in order to realise the full potential of operational synergies between Europol and FIUs, the network facilitating information exchange between FIUs (FIU.NET) will be replaced by SIENA and the services of the FIU.NET Bureau will be fully embedded within Europol (including the staff of the FIU.NET Bureau). Remaining details around governance, data processing and FIU activities will be addressed with view to achieving more operational added value from linking general money flows to criminal activities and following up to identified links.[156]

The embedment process took effect in January 2016 and a Service Level Agreement, outlining how Europol was to sustain the FIU.net was concluded in October of the same year.[157] FIUs are connected to Europol through the Europol National Units.[158] Needless to say, the embedment process proved both legally and technically complicated and a lot of obstacles emerged along the way - even before the EDPS delivered the final blow. More specifically, the FIU.net's *full* integration with SIENA (that is, replacing the network by SIENA) that was referred to in the Common Understanding, proved very challenging – which is why the FIUs Platform and Europol agreed to proceed in smaller steps, and considered whether interoperability between FIU.net and SIENA might be a more appropriate first step.[159]

---

154 EDPS, 'Annual Report 2019', 41.

155 European Parliament, Parliamentary Questions (n 86).

156 Europol, 'Work Programme 2013', (The Hague, 11 July 2012), 23. SIENA, which stands for 'Secure Information Exchange Network Application', is Europol's secure communication system.

157 Europol, '2017 Consolidated Annual Activity Report', (The Hague, 1 May 2017), 36.

158EU FIUs Platform (n 90).

159 EU FIUs Platform, 'Minutes of the 31st Meeting of the EU FIUs Platform' (11 March 2017).

In any event, and given that FIU.net had to be upgraded as a system, Europol presented in 2017 a proposed Roadmap for the network's future.[160] The proposal envisaged a move towards a *centralised* system (recall that FIU.net is a decentralised network) and in particular towards centralised sharing but decentralised matching of information.[161] On that note, some participants of the Platform raised concerns about retaining control of their own data.[162] In response to that, Europol remarked that it is a *cooperation partner* (which meant that it was up to FIUs to choose whether to share information with Europol), but also *a service provider* at the same time – and that the proposed Roadmap 'does not suggest that FIUs give access to each other's databases (even if FIU at some point in time would like to share more information) or act against their national data protection rules'.[163]

Some FIUs, however, did not view the proposal positively and raised a series data protection concerns – mainly around storage of data, noting that the Fourth anti-money laundering Directive 'does not provide the legal basis to transfer STR data to a database other than an FIU one.[164] In other words, some FIUs stressed out that during the 'analysis' phase, data from suspicious transaction reports can only be shared between FIUs; in their view, unless the FIU decides (following its analysis) that the suspicion is indeed substantiated and that the information must be shared with law enforcement, data can only travel from FIU to FIU and cannot be stored at a law enforcement database (such as Europol's).[165]

In light of those objections, Europol and FIUs begun working towards a revised Roadmap, but they also sought the advice of the EDPS and the Europol Cooperation Board[166] on the data protection issues that were raised.[167] Interestingly, it was *not* the processing of data by Europol in its capacity as a cooperation partner that raised concerns for the EDPS; rather, it was the processing of data in its capacity as a service provider and technical administrator of the FIU.net. More specifically, the issue was whether the processing of FIU data that accompanied the maintenance of FIU.net complied with the data processing requirements of the Europol Regulation.

---

160 EU FIUs Platform (n75).

161 ibid.

162 ibid.

163 ibid.

164 EU FIUs Platform, 'Minutes of the 34th Meeting of the EU FIUs Platform' (6 March 2018).

165 ibid.

166 The Cooperation Board is composed of a representative of a national supervisory authority of each Member State and of the EDPS. See Article 45, Regulation 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) [2016] OJ L 135/53 (Europol Regulation).

167 Europol Cooperation Board, 'Activity Report 2017-2018', 6.

According to that Regulation, Europol may process personal data for the purposes of:

a) cross-checking aimed at identifying connections or other relevant links between information related to:

i. persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;

ii. persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent;

b) analyses of a strategic or thematic nature;

c) operational analyses;

d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.[168]

Annex II of the Europol Regulation further lists the specific categories of personal data that may be processed for the above purposes.[169] The maintenance of FIU.net arguably falls under d) – facilitating information exchanges. The key question, therefore, is whether the processing of FIU data in this context falls within the categories of data that may be collected and processed for the purposes of facilitating information exchange, as listed by Annex II of the Regulation.[170] According to this list, such personal data must relate to (among others) 'persons who, pursuant to the national law of the Member State concerned, are *suspected* of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence.'[171]

It is the word 'suspected' that brings us to the heart of the matter. FIUs deal with suspicious *transaction* reports - but that doesn't necessarily mean that they deal with *suspects*. According to the EDPS, for Europol to comply with the aforementioned requirements, the individuals involved in suspicious transactions would have to qualify as 'suspects'.[172] But, as he rightly pointed out, FIUs 'act before the start of any criminal proceeding or investigation has begun'.[173] The Europol Regulation does not define 'suspect' – this is a matter of national law. In light of this, the Europol Cooperation Board issued an opinion in September 2019, which advised that FIU.net could not benefit from Europol's technical infrastructure, because the categories of data processed 'do not seem consistent with Europol's mandate'.[174] Following that,

168 Article 18 (2), Europol Regulation.
169 Article 18 (5), Europol Regulation.
170 Annex II (B), Europol Regulation (emphasis added).
171 ibid.
172 EDPS (n 154).
173 ibid.
174 Europol Cooperation Board, 'Report to the Joint Parliamentary Scrutiny Group' (23 September 2019).

the EDPS published its decision in December of the same year; he concluded that the data processing carried out by Europol in the context of the technical operation of the FIU.net breached the Europol Regulation and therefore, he imposed a ban on those processing operations.[175] Given the importance of FIU.net for information exchanges between EU FIUs, the ban was suspended until December 2020, to allow time for moving FIU.net to another host organisation.[176]

In other words, Europol, in its capacity as a technical administrator of FIU.net, has been processing FIU data in the absence of a legal basis that enabled it to do so – in breach of the Europol Regulation. This is one more instance where the need to secure an operationally convenient arrangement for information exchanges side-lined data protection considerations.

Conclusion

FIUs may belong in the broader 'policing' sphere, but in reality, they are stuck in the middle between the (former) first and third pillars. They might have been established by a first pillar instrument (the AML Directive), but their functions are more closely connected to the field of crime prevention rather than the internal market. The 'grey zone' where FIUs operate has generated significant difficulties in determining the data protection instrument that should govern their domestic activities. Some FIUs are governed the GDPR, while others by its law enforcement counterpart. And this choice is not necessarily determined by the nature of the FIU. As we saw, there are police FIUs who apply the GDPR. In this article I have argued that, contrary to the Commission's opinion, the Police Data Protection Directive is a more appropriate legal framework for them. Currently, FIUs are holding discussions under the umbrella of the EU FIUs Platform on this matter – and it seems that several Member States have subjected their FIUs to the Police Data Protection Directive. But so long as these divergencies exist, there is an uneven playing in field in the protection guaranteed to the personal data of individuals.

It is not just the quality of the FIU nature that is ambiguous. Their activities, too, evolved in a piecemeal manner – even more so when it comes to their transnational activities. As we saw, the transfers of data between them are regulated by multiple instruments. If we add to that

---

175 That opinion has not been made public for security reasons.

176 ibid. In June 2020, the Council called on the Commission 'to table a proposal for a long-term solution for FIU.net or its successor that will ensure effective cooperation between FIUs, as well as between the FIUs and Europol'. See Council of the EU, 'Council conclusions on enhancing financial investigations to fight serious and organised crime' (Brussels, 17 June 2020), Document 8927/20, 9.

the uncertainty over the data protection framework that applies to their cooperation, the persistent calls for maximum information exchange, and the novel forms of FIU cooperation envisaged by the EU legislator, it becomes clear that FIU cooperation presents several challenges for the protection of personal data. A first step to overcoming them would be to clarify the data protection framework that should be applicable to their transnational activities.

But this is not the only challenge from a data protection perspective. As the example of FIU.net's integration into Europol illustrated, when policymakers are fixated with improving the operational cooperation of EU FIUs, data protection considerations may easily fall through the cracks. Europol was processing FIU data in its capacity as the technical administrator of the FIU.net since 2016, in the absence of a legal basis for that processing – in breach of the Europol Regulation. But given the large amounts of personal and financial data that is regularly exchanged between EU FIUs, data that also belong to innocent individuals, data protection should not be side-lined.