Enhancing AML/CTF through Private Sector Data Exchange: What Opportunities Does Art. 75 of the New EU Money Laundering Regulation Offer for Collaborative Transaction Monitoring?

*by Prof. Dr. Kilian Wegner**

I. Introduction

It is commonly known that private entities can fulfill their AML/CTF due diligence obligations much more effectively and efficiently if they do not have to rely only on their own data, but also receive information from other obliged entities (or even from government agencies like the police). This is particularly evident in transaction monitoring, where it is very hard for a single financial institution to recognize risks in payment transactions that go beyond the most obvious solely based on the customer data and transaction data available in the institution.[1] Collaborative transaction monitoring[2] offers at least two use cases here:

---

* Kilian Wegner is an Assistant Professor for Criminal Law, Criminal Procedure and White-Collar Crime @ European University Viadrina Frankfurt (Oder) and Editor-in-Chief of the German Journal "Geldwäsche & Recht / Money Laundering & Law". He is also a member of the expert panel of the German Anti-Financial-Crime Alliance (AFCA)

1 This article will therefore focus on collaborative transaction monitoring, but that is not to say that private-to-private data sharing does not have potential in other areas as well (for example when it comes to BO data in jurisdictions that do not [yet] have a central BO register), see *pars pro toto* FATF, Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing., July 2022 (available online via https://t1p.de/2vi34), pp. 11 seq.

2 The term „collaborative transaction monitoring" is borrowed from *Maxwell*, who defines it as a system where two or more members (typically financial institutions) are pooling or connecting transaction data (or, potentially, only transaction alerts) to be able to analyse risks that span across multiple financial institutions (see *Maxwell*, A Survey and Policy Discussion Paper: "Lessons in private-private financial information sharing to detect and disrupt crime", July 2022, available online via https://t1p.de/7a0r6, p. 34).

- On the one hand, it can be used to discover previously unknown risks by following payment flows across institutions.[3] One example of an "unknown unknown" that can be discovered in this way are suspicious network structures such as circular transactions. Another interesting option is to propagate risk scores along payment flows.[4]
- On the other hand, collaborative transaction monitoring can be used to assess the scope of risks that have already been identified.[5] The range of data one can share for this purpose extends from mere statistical information (e.g. on averaged risk scores on counterparties of one's own customers) to openly exchanged operational information (e.g. when a bank has carried out investigations into the economic background of a payment sender and shares the results with banks whose customers have received comparable payments from the same sender).

For years, attempts have therefore been made worldwide to strengthen data sharing between obliged entities, of which the projects based on Section 314 (b) of the Patriot Act, such as the *Nasdaq Verafin* platform, are probably the longest-standing focusing specifically on money laundering and terrorist financing.[6] As *Maxwell* has shown meticulously in two studies,[7] the existing projects differ considerably in terms of which data (personal data or only business data, pre- or only post-suspicion data etc.) is shared between which actors, in which process and in which encryption mode.

---

3 This is an objective that for example was originally pursued by the Dutch TMNL project (which will be mentioned in more detail later).

4 For more about this see *Van Egmond et. al.*, Cryptology ePrint Archive Paper 2024/64 (available online via https://t1p.de/3chwr).

5 The Swiss AML Utility project, for example, is moving in this direction.

6 See *Maxwell* (Fn. 2), pp. 26 seq. for even older projects in the fraud area and for the historical development of private-to-private data sharing to combat financial crime as a whole.

7 *Maxwell* (Fn. 2) and *Maxwell*, Expanding the Capability of Financial Information-Sharing Partnerships, March 2019, available online via https://t1p.de/g5ctl.

While the sharing of **strategic information** – such as typology reports – has steadily increased over the past years, often facilitated through public-private partnerships (PPP), a broad breakthrough in the exchange of **operational data** (e. g. transaction data) has not yet materialized in Europe or elsewhere, although there are examples of such undertakings, one of which is the Dutch TMNL project (more on this in a later section). The underlying reluctance of potential participants is (among other reasons) due to the at least unclear legal framework and the strong position that data protection in particular plays in the EU. Finding technological ways to accommodate those on data handling – which are set up for instance by the EU General Data Protection Regulation (GDPR), but also by the ban on tipping off under money laundering law or restrictions on cooperation under antitrust law – pose a risk only few obliged entities are willing to take. In recent months many have expressed the hope that the regulatory uncertainty could change because of the creation of Art. 75 of the new EU Anti-Money Laundering Regulation (EU-AMLR),[8] as this provision provides for the first time an explicit legal basis for the exchange of data between AML/CTF obliged entities applicable all over the European Single Market. In this paper, I will examine whether these hopes for a clear legal basis are justified and under which conditions data sharing utilities (using the example of collaborative transaction monitoring) can be operated based on Art. 75 EU-AMLR, while also discussing issues that might be inherent to the new regulation.[9]

II. Eligible parties for data sharing based on Art. 75 EU-AMLR

Art. 75 Abs. 1 EU-AMLR permits the exchange of data within the scope of so-called **partnerships for information sharing**. All obliged entities (in addition to public bodies

---

8 Regulation (EU) 2024/1624 of the European Parliament and the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, available online via https://t1p.de/9qjvv.

9 A similar objective is pursued by *Cusack* in his contribution on Financial Crime News from May 10th 2024, available online via https://t1p.de/qkd9k.

such as the FIU) can participate in such a partnership. There is no restriction to obliged entities in the financial sector. The partnership can also be cross-border.

III. What types of data can be shared under Art. 75 EU-AMLR?

1. Broadly defined scope in Art. 75 para. 3 subpara. 1 EU-AMLR

Art. 75 para. 3 subpara. 1 EU-AMLR describes a broad scope of data that can be exchanged within the framework of partnerships for information sharing and also permits the exchange of **tactical / operational information**, in particular customer data (address, name etc.), transaction data, CDD data (such as risk classification) and TM data (number of alerts etc.). Contrary to what is sometimes assumed, the text of the regulation **does not** contain any restriction to **post-suspicion data**. The law literally deems the following data types suitable for sharing in Art. 75 para. 3 sentence 1 EU-AMLR:

- information on the customers, including any information obtained in the course of identifying and verifying the identity of the customer and, where relevant, the beneficial owner of the customer;
- information on the purpose and intended nature of the business relationship or occasional transaction between the customer and the obliged entity, as well as, where applicable, the source of wealth and source of funds of the customer;
- information on customer transactions;
- information on higher and lower risk factors associated with the customer;
- the obliged entity's analysis of the risks associated with the customer pursuant to Art. 20 para 2 EU-AMLR;[10]

[10] Art. 20 para. 2 EU-AMLR reads as follows: *"Obliged entities shall determine the extent of the measures referred to in paragraph 1 on the basis of an individual analysis of the risks of money laundering and terrorist financing having regard to the specific characteristics of the client and of the business relationship or occasional*

- information held by the obliged entity pursuant to Art. 77 para. 1 EU-AMLR;[11]
- information on suspicions pursuant to Art. 69 EU-AMLR.[12]

2. Restriction of data sharing to high-risk cases by Art. 75 para. 4 lit. f) EU-AMLR?

While Art. 75 para. 3 subpara. 1 EU-AMLR seems to be constructed to permit wide application, the scope of data permitted for exchange is then narrowed (at least at first glance) by Art. 75 para. 4 lit. f) EU-AMLR. This paragraph literally states under i) and ii) that only data of customers may be exchanged,

- *"whose behaviour or transaction activities are associated with a higher risk of money laundering, its predicate offences or terrorist financing, as identified pursuant to the risk assessment at Union level and the national risk assessment carried out in accordance with Articles 7 and 8 of Directive (EU) 2024/1640"*

  or[13]

- *"who fall under any of the situations referred to in Articles 29, 30, 31 and 36 to 46 of this Regulation."*

---

transaction, and taking into account the business-wide risk assessment by the obliged entity pursuant to Article 10 and the money laundering and terrorist financing variables set out in Annex I as well as the risk factors set out in Annexes II and III."

11 According to Art. 77 para. 1 EU-AMLR ("Record retention") obliged entities shall retain the documents and information specified in the wording of the paragraph (such as a copy of the documents and information obtained in the performance of customer due diligence). Such documentary evidence may be shared within a partnership in the sense of Art. 75 EU-AMLR.

12 Art. 69 EU-AMLR contains the duty to report suspicions to the FIU.

13 As far as *Cusack* (Fn. 9) raises the question of whether the conditions set out in Art. 75 para. 4 lit. f) (i) and (ii) EU-AMLR are alternative or cumulative, the answer is clear: since the legislator has linked (ii) and (iii) with an "or", all three letters are to be understood as alternative conditions in accordance with the usual structure of EU law.

If one follows the references to provisions into the Directive 2024/1640 (= EU-AMLD) and into Art. 29, 30, 31 and 36 to 41 EU-AMLR, the following transaction types or customer groups can be identified for which data exchange is permitted in accordance with Art. 75 para. 4 lit. f) i) and ii) EU-AMLR:

- Transactions or business activities which, according to the **supranational risk analysis of the EU Commission**,[14] are associated with a higher risk of money laundering or terrorist financing;[15]
- Transactions or business activities that are associated with a higher risk of money laundering or terrorist financing according to the **national risk analysis** in the country of domicile of the obliged entity contributing to the data;[16] depending on the scope and level of detail of the respective national analysis, the list of activities classified as "high risk" on this path can be **very broad**;
- Customers based in **high-risk countries** according to EU classification;[17]
- Customers based in countries to which the EU Commission attributes **compliance weaknesses in their national AML/CFT regime**;[18]
- Customers domiciled in countries that the EU Commission considers to pose a **specific and serious threat to the EU's financial system**;[19]

14 Last version of October 27, 2022, available online at https://t1p.de/wu5df.
15 Art. 7 EU-AMLD.
16 Art. 8 EU-AMLD.
17 Art. 29 EU-AMLR.
18 Art. 30 EU-AMLR.
19 Art. 31 EU-AMLR.

- Customers in **cross-border correspondent banking relationships**[20] and comparable correspondent relationships;[21]
- Customers who receive crypto values from or send them to **self-hosted wallets**;[22]
- Customers seeking a **"golden passport"**;[23]
- Customers who have the status of a **politically exposed person (PEP)**.[24]

In the academic literature, the restrictions of Art. 75 para. 4 lit. f) i) and ii) EU-AMLR have sometimes been summarized in such a way that the exchange of data pursuant to Art. 75 EU-AMLR is only permissible for high-risk transactions or high-risk clients.[25] However, this fails to recognize that in addition to Art. 75 para. 4 lit. f) i) and ii) EU-AMLR, there is also **Art. 75 para. 4 lit. f) iii) EU-AMLR**. Alternatively to lit. i) and ii), lit. iii) also permits the exchange of data when customers are involved *„for whom the obliged entities need to collect additional information in order to determine whether they are associated with a higher level of risk of money laundering, its predicate offences or terrorist financing"*.

This wording appears to be the result of a compromise, which is typical of the trilogue negotiations between European Commission, European Parliament and the Council of the European Union in which EU regulations are created: The decision taken in Art. 75 para. 4

---

20 A correspondent banking relationship is an arrangement between two banks, typically in different countries, where one bank (the correspondent bank) provides services such as payments, deposits, and foreign exchange to the other bank (the respondent bank) to facilitate international financial transactions on behalf of the respondent bank's clients. This relationship enables the respondent bank to access financial services in markets where it does not have a physical presence. This arrangement carries a higher AML risk because the correspondent bank often processes transactions for customers of the respondent bank without direct knowledge of those customers, creating opportunities for money laundering or other illicit activities to occur through complex cross-border transaction chains, especially in jurisdictions with weaker regulatory oversight.

21 Art. 36–39 EU-AMLR.

22 Art. 40 EU-AMLR.

23 Art. 41 EU-AMLR.

24 Art. 42 seq. EU-AMLR.

25 See for example *Brana/Bostock/Cundall*, Article 75: A new opportunity to fight crime more effectively, October 2024 (available online at https://t1p.de/o0snf), p. 10.

lit. f) i) and ii) EU-AMLR to restrict the data to the high-risk area was probably difficult to agree on, which is why it is directly counteracted by the relatively open clause in lit. iii). After all, the wording **"additional information"** used in the clause allows a customer to be included in data sharing even if there is the slightest indication of a high risk. Strictly speaking, it cannot really be ruled out with any customer that "additional information" could lead to the customer being classified as a high-risk customer. If the provision is interpreted in this way, Art. 75 para. 4 lit. f) EU-AMLR on closer inspection does not result in any restrictions with regard to what data can be shared.[26]

By creating this friction between Art. 75 para. 4 lit. f) i) and ii) EU-AMLR on the one hand and Art. 75 para. 4 lit. f) iii) EU-AMLR on the other hand, the trilogue partners have thus ultimately left the legal policy decision on the extent to which data may be shared in accordance with Art. 75 EU-AMLR to be shaped by practice and, in the final instance, by the courts.

IV. Which method can be used to share data in accordance with Art. 75 EU-AMLR?

Art. 75 para. 1 EU-AMLR states that obliged entities may share information "among each other". If interpreted very narrowly, this could be understood to mean that only the **bilateral** exchange of information between obliged entities or models with decentralized data analysis are covered, but not the feeding of data into a **centralized data pool**. However, the wording of the provision is by no means mandatory in this respect. The historical context of Art. 75 EU-AMLR also speaks against the narrow interpretation: Parliament and Council wanted to place the existing European projects for horizontal data exchange on a solid legal basis in order to make data exchange more widespread.[27] Since

---

26 See for possible interpretations of Art. 75 para. 4 lit. f) iii) also *Cusack* (Fn. 9).

27 C. f. recital 146 and 147 of the EU-AMLR*: "Criminals move illicit proceeds through numerous intermediaries to avoid detection. Therefore it is important to allow obliged entities to exchange information not only between group members, but also in certain cases between credit institutions and financial institutions and other entities that operate*

the vast majority of existing projects are based on a form of data pooling, it would run counter to the legislative intention to exclude data pooling models from Art. 75 EU-AMLR.

Finally, data pooling models for data exchange do not violate the **rules on outsourcing due diligence measures** contained in the EU-AMLR. Not only does Art. 18 para. 1 EU-AMLR in principle allow the assignment of monitoring tasks to a pool service provider, but Art. 18 para. 3 sentence 2 lit. f) EU-AMLR makes it clear that the determination of the monitoring criteria may also be outsourced to the service provider as long as the responsibility for the *approval* of these criteria remains with the obliged entity.[28] Art. 18 para. 3 sentence 2 lit. c) EU-AMLR is also not an obstacle, because even in the case of collaborative transaction monitoring by way of a central pool solution, the decision as to which risk profile is to be assigned to a customer remains with the obliged entity, who is only taking into account the collaborative analysis results.[29]

V. What privacy measures must be taken when exchanging data in accordance with Art. 75 EU-AMLR?

If several obliged entities exchange data for the purpose of ML/TF prevention, this may constitute a serious interference with the right to privacy of the customers concerned (and

within networks, with due regard to data protection rules. […] The exchange of information among obliged entities and, where applicable, competent authorities, might increase the possibilities for detecting illicit financial flows concerning money laundering, the financing of terrorism and proceeds of crime. For that reason, obliged entities and competent authorities should be able to exchange information in the framework of an information sharing partnership where they deem such sharing to be necessary for compliance with their AML/CFT obligations and tasks. […]".

28 Art. 18 para. 3 sentence 2 lit. f) EU-AMLR also shows once again the legislator's intention to allow centralized data pooling solutions to continue. In the original Commission draft of the EU-AMLR, Art. 40 para. 2 lit. e) (which today essentially is Art. 18 para. 3 sentence 2 lit. f) EU-AMLR) stated that the definition of monitoring criteria is generally inadmissible – effectively a death sentence for the use of pooling service providers for data exchange (*Seehafer*, GWuR 2022, p. 135, 140 had pointed this out). The fact that the trilogue partners have amended the provision to its current version can be interpreted as a decision in favor of collaborative transaction monitoring by central service providers.

29 In this respect, see also *Seehafer*, GWuR 2022, 135, 140.

their transaction partners).[30] It should therefore come as no surprise that such data exchange within the European Union must meet the requirements of the **EU General Data Protection Regulation** (GDPR) – the introduction of Art. 75 EU AMLD does not change this. Against this background, there has been much discussion in recent years about the extent to which the impairment of privacy associated with data sharing can be mitigated by the use of so-called **privacy preserving technologies (PET)**. Hidden behind this colorful term are very different technological approaches, ranging from simple pseudonymization of data to complex cryptographic methods such as **secure multi-party computation**, in which several parties can jointly perform analyses of their combined data, while the data always remains encrypted and fragmented, so that no party has access to the information of the other parties.[31]

What all these technologies have in common is that they are only "privacy preserving" in the sense that the data fed into the system by one system participant (such as a bank) is not disclosed openly to other system participants. However, PETs do not change the fact that the people linked to the encrypted data are subject to monitoring and therefore surveillance.[32] And this surveillance is all the more effective (from a prevention perspective) or intrusive (from a fundamental rights perspective) the more obliged entities participate, regardless of the technology used. It is therefore important not to be tempted to believe that the problem of balancing prevention efficiency and data protection is completely

---

30 An in-depth legal assessment of collaborative transaction monitoring on the basis of the GDPR and the data protection case law of the European Court of Justice (ECJ) is provided by *Seehafer*, GWuR 2022, pp. 135 seq.

31 See *Van Egmond et. al.*, Cryptology ePrint Archive Paper 2024/64 (available online via https://t1p.de/3chwr).

32 Exceptions to this are technologies that completely anonymize data so that it is impossible to draw conclusions about individual persons. However, the use of anonymous customer and transaction data for the purpose of ML/TF prevention will only make sense in a few situations. For example, it would be conceivable to use this kind of data if the aim was simply to collect as much data as possible to create a better benchmark for an anomaly check on transactions. In this case, it is irrelevant whether the transaction or customer data included in the benchmark can ever be assigned to a specific person again.

solved by the use of PETs. Rather, the processing of transaction data using PETs remains **data processing** within the meaning of the GDPR. This means (*inter alia*) that the principle of data minimization laid down in the GDPR must be observed in the context of the exchange of information based on Art. 75 EU-AMLR and that an appropriate balance must be found between the impact on privacy on the one hand and the benefits for AML prevention on the other.

Unfortunately, anyone looking for references to the balancing problem outlined above in the wording of Art. 75 EU AMLD will not find them. Avoiding any fundamental decision on this, the legislator merely states in Art. 75 para. 4 lit. e) EU-AMLR that *"obliged entities shall implement appropriate technical and organisational measures […] to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged"*. As an example of such measures, the pseudonymization of data is mentioned. About PETs the law does not say a word. Art. 75 EU-AMLR thus provides the reader with nothing more than an open formula for weighing up the conflicting interests without a clear foothold. This is precisely where further debate must begin. In my view, a sensible idea would be to underpin Art. 75 EU-AMLR with a kind of "ladder" model, which can be sketched as follows:

- The **first stage** of the ladder involves the participants in a data exchange partnership using **secure multiparty computation** to share **statistical information** on transaction data without disclosing the names of the financial institutions involved. For example an obliged entity could receive information about how many high risk counterparties a client has in this network and how many of those counterparties have transactions larger than X or transactions involving high risk jurisdiction. Sharing statistical information like this makes it unlikely that conclusions can be drawn about individuals, but still provides insights about the network of a client and whether he is part of a low or a high risk network. Since the exchange of such information only slightly interferes with the privacy of the customers concerned

(and their business partners), it should always be permitted, even on a large scope of data.

- The **second stage** of the ladder involves sharing **more granular statistical data** among the participants in a data exchange partnership. At this level, secure multiparty computation is still employed to protect sensitive information, but the data shared is more detailed and carries a higher risk of accidently revealing individual identities. Examples of such data include the specific transaction amounts, detailed account activity patterns, or timing of transactions that deviate from the usual behavior of similar customers. Furthermore, data on transaction relationships (such as frequent interactions between accounts with a known high-risk profile) or linked accounts involved in suspicious activities may also be shared. While the increased granularity of this data poses a higher risk of identifying individuals or institutions, its exchange can be justified when it is necessary for targeted AML investigations. However, due to the potential privacy concerns, such exchanges should be limited to high-risk cases.

- The **third stage of** the ladder involves the **open exchange** of personal data (names, account details, specifics of transactions in question etc.) between obligated entities, a step that carries significant privacy risks due to its direct impact on privacy. This stage is reserved for situations where the risk profile of a customer or transaction has become so pronounced that the participating entities believe that, possibly subject to consideration of the results of the data exchange, they are compelled to file a suspicious transaction report.

It is obvious that not every case constellation can be clearly fitted into such a "ladder" model and that the transition between the exchange of purely statistical data and the exchange of open data can be fluid depending on the choice of data. Nevertheless, I believe that such a model gives the obliged entities more guidance than an open formula such as

that contained in the current wording of Art. 75 EU-AMLR. Looking at compability with the GDPR I think it is decisive that the model makes it possible to analyze a large majority of transactions using multi-party computation in the most privacy-preserving way possible (level 1 and 2) and to have an open data exchange only in those cases where this is absolutely necessary (level 3). The model can therefore help to bring the principle of data minimization to concrete fruition when applying Art. 75 EU-AMLR.

This leads to the question of who could design such a "ladder" model in practice. According to Recital 148, the EU-legislator appears to have assumed that specifications of Art. 75 EU-AMLR could be developed by the individual Member States.[33] It would, however, be far more sensible if the discussion in this regard were channeled through the newly established EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). While Art. 75 EU-AMLR does not directly provide AMLA with the authority to further specify data exchange under Art. 75 through a Regulatory Technical Standard (RTS) or through guidelines, the provisions on data exchange are inextricably linked to the due diligence measures for which data exchange is necessary. Consequently, AMLA should, for example, have the ability to incorporate detailed rules for collaborative transaction monitoring within the guidelines on transaction monitoring based on Art. 26 para. 5 EU-AMLR. Of course, this does not mean that obliged entities would have to wait until the AMLA or other authorities have gone ahead before implementing data sharing utilities, as Art. 75 EU-AMLR is directly applicable as the legal basis for the exchange of information from 2027 without the need for further concretizing legal acts. It would certainly be ideal if public and private impetus to bring Art. 75 EU-AMLR to life went hand in hand.

33 *„Consistent with Regulation (EU) 2016/679, Member States should be able to maintain or introduce more specific provisions to adapt the application of that Regulation to provide more specific requirements in relation to the processing of personal data exchanged in the framework of a partnership for information sharing."*

VI. The motivational moment: Why should obliged entities participate in data sharing at all?

The trilogue partners seem to have tacitly assumed, in creating Art. 75 EU-AMLR, that obliged entities have an intrinsic motivation to participate in partnerships for information sharing as there is no explicit obligation for such participation to be found in the regulation. This may prove to be a stumbling block for large-scale implementation of data sharing partnerships in practice, as the benefits of data sharing for obliged entities highly depend on the use case. For some applications, the benefits are clear for example, when it comes to reducing KYC costs through pooled information on individuals' PEP status or pooled long-distance identification facilities. In transaction monitoring, there is mixed picture: While voluntary additional efforts to detect risks with collaborative transaction monitoring that would not be visible with legally required due diligence ("unknown unknowns") might not be an attractive business case for all obliged entities, the use of collaborative transaction monitoring to assess risks that have already been identified has considerable potential for cost savings since it allows a more targeted and informed decision to be made on which transactions more resources should be used for analysis and for which less. Cost savings are expected in particular in investigations (e.g. in the context of enhanced due diligence obligations), as collaborative transaction monitoring allows an accurate assessment of when investigative cooperation with another obligated entity is promising and can significantly shorten the investigation process.[34]

The fact that collaborative transaction monitoring is not a self-runner can be seen in the example of the Dutch Transactie Monitoring Nederlands (TMNL) mentioned at the

---

[34] Consider, for example, the situation in which a bank has submitted a suspected money laundering report with regard to a transaction and, in the course of a follow-up investigation, receives investigation results from another bank via data sharing, which show that the transaction was actually harmless. The bank could thus justifiably refrain from carrying out further enhanced due diligence with regard to this customer (as is normally necessary after submitting a SAR) and thus save considerable costs.

beginning of this text. Despite significant investments by participating banks and reportedly substantial successes in detecting complex money laundering and tax evasion schemes (as evidenced by internal, as yet unpublished, reports), the project was discontinued in early July 2024, and most employees were laid off. The official reason cited on the TMNL website for the project's termination is compliance with Art. 75 EU-AMLR, which will apply starting in 2027, necessitating technological restructuring.[35] However, this explanation is not completly convincing. First, several years remain before Art. 75 EU-AMLR, which will apply from 2027 onwards, comes into effect. Second, it is unclear why Art. 75 EU-AMLR, in principle, would prevent the continuation of the TMNL approach. Admittedly, it is true that the original approach of the TMLN project to uncover previously unknown money laundering risks by means of network analysis would be made considerably more difficult if Art. 75 EU-AMLR were to be interpreted narrowly and only "high-risk" data were to be shared rather than all transaction data. However, as shown above, it is not at all clear whether this narrow interpretation will prevail and, on the other hand, it would have been possible to adapt the project to these strict requirements (for example, by focusing the data analysis on risk assessment rather than risk detection).

Speaking with people involved behind the scenes, it becomes clear that differing interests and motivations among the banks participating in TMNL may have played a role in the decision to (at least temporarily) discontinue the project. Political opposition (among others by the Dutch Data Protection Authority Autoriteit Persoonsgegevens[36] and the so-called

---

35 See https://tmnl.nl/en: *„In preparation for the implementation of new European legislation (AMLR) in July 2027, TMNL is adjusting its operations and business model. To comply with this regulation, TMNL will scale down its current activities and restructure them in collaboration with its partners. This means that TMNL, in its current form, will cease to exist".*

36 See, for example, the letter from the AP to the Dutch Ministry of Finance dated July 14, 2023, available online via https://t1p.de/dtcvr.

Human Rights in Finance Foundation[37]) and uncertainties in Dutch law,[38] that were supposed to be eliminated by the anti-money laundering package "Plan van aanpak witwassen"[39], which however has not yet been passed, will certainly also have influenced some decision-makers, fostering a "don't dare to share" attitude.

Looking at examples like this, it would be naive to assume that collaborative transaction monitoring (and similar applications of data sharing) will automatically gain widespread implementation as soon as Art. 75 EU-AMLR establishes a (still unclear) legal framework for it – and that is although there are good prospects of significantly reducing the costs incurred by financial institutions due to false positive alerts in transaction monitoring, for example. Rather, what will likely be required is that the involved government agencies take on a leadership role in this area.[40] As mentioned above, the AMLA, in conjunction with FIUs, seems to be particularly well-positioned to take on this role. In the short term, these authorities will need to extract a workable operational framework from the vague wording of Art. 75 EU-AMLR. This will encourage many obligated entities to experiment with the cost-cutting potential of collaborative transaction monitoring. If, on the other hand, the aim is to use collaborative transaction monitoring to uncover "unknown unknowns" (which tends to increase costs and is therefore not in the intrinsic interest of the obligated parties), the focus must be set on shifting data sharing from a purely voluntary supplementary measure to an obligation in the long term. The broadly worded due diligence provisions in Art. 19 seq. provide sufficient room for this. Why should the AMLA, for example, not at

---

37 The Human Rights in Finance Foundation (HRIF) has been campaigning against the TMNL project for years, see the report by RiskCompliance of July 16th, 2024, available online at https://t1p.de/r19rc. In a legal opinion commissioned by the HRIF published in Juli 2024 (available online at https://t1p.de/d868l), the Dutch law firm Prakken d'Oliveira even accuses the TMNL to be a criminal endeavour.

38 There is a dispute, for example, about the interpretation of the (partial) prohibition of outsourcing contained in Art. 10 Wwtf (Wet ter voorkoming van witwassen en financieren van terrorisme), see the report by RiskCompliance cited in Fn. 34.

39 The initial proposal can be found online via https://t1p.de/ow212.

40 That the public sector should play an active role in facilitating private-to-private data sharing is also recommended by the FATF, see the report in Fn. 2, pp. 51 seq.

some point in the future provide in its guidelines pursuant to Art. 26 para. 5 EU-AMLR that certain transactions are only sufficiently "monitored" within the meaning of Art. 26 para. 1 EU-AMLR if the monitoring is carried out via collaborative transaction monitoring?

VII. Summary

Anyone expecting the EU-AMLR to provide a clear regulatory framework for the exchange of data between obliged entities in the AML/CTF area is bound to be disappointed after reading Art. 75 EU-AMLR. Certainly, the provision contains the welcome decision that the exchange of data between obliged entities is generally permissible and this explicitly also applies to operational data, for example for the purpose of KYC or transaction monitoring. However, central questions – such as whether the exchange is limited to transactions or customers with a certain risk profile or whether and how data must be encrypted while in use – could obviously not be clarified in the legislative trilogue procedure. In this respect, large parts of Art. 75 consist of cloudy compromise formulas, which are ultimately more a suggestion for further discussion than a clear legal basis. Certainly, this can also be an opportunity to develop a technically sensible and at the same time politically tenable interpretation of the regulation in practice. With this freedom of design, however, comes a considerable responsibility to make it clear to the public and ultimately to the European Court of Justice, which will at some point decide on the limits of data sharing under Art. 75 EU-AMLR, that an effective *data sharing* approach offers a (the?) chance to overcome the current malaise of AML/CTF prevention (not only) in Europe. This applies particularly to transaction monitoring, for which the triad of "primitive", "expensive" and "unsuccessful" would still be a diplomatic description of the status quo. The debate about when and for what reasons it is acceptable that operational customer and transaction data may (and possibly must) be shared in a procedure to be defined in more detail should therefore be conducted urgently and intensively.