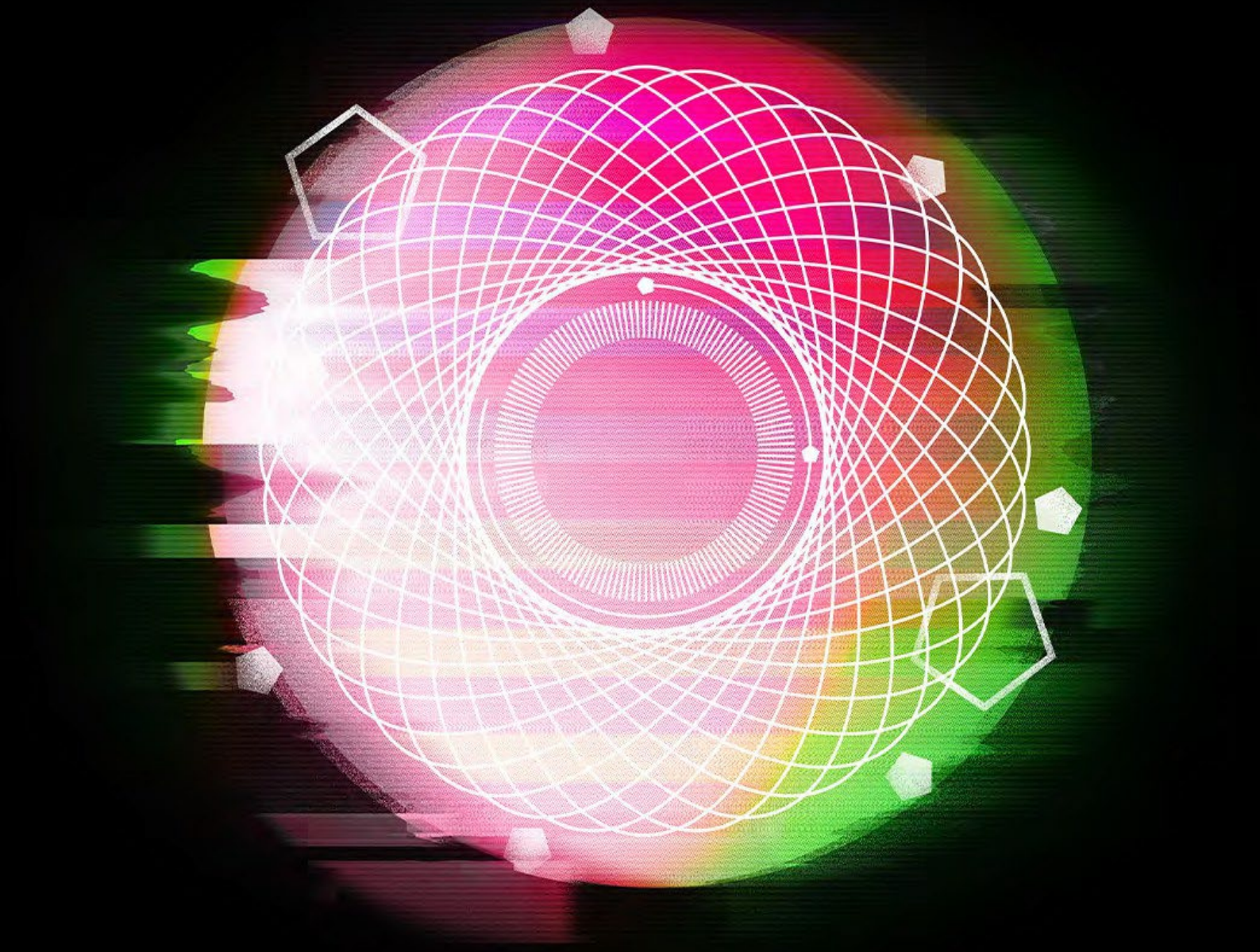
Deloitte.



Article 75: A new opportunity to fight crime more effectively

October 2024

MAKING AN IMPACT THAT MATTERS since 1845

Contents

1. Introduction 3

2. Why was Article 75 created? 4

3. Article 75: an overview 5

4. Establishing a partnership for information sharing under Article 75 7

5. The potential value of Article 75 9

6. Does Article 75 go far enough? 10

7. Conclusion 12

1. Introduction

Global illicit financial flows are substantial. NASDAQ estimates that $3.1 trillion in illicit funds flowed through the global financial system in 2023[1]. The United Nations estimates that the erosion cost to governments (i.e., in lost tax revenues) from money laundering is around $1.6 trillion[2]. The response is substantial too, with the total cost of financial crime compliance in EMEA estimated at $85 billion[3]. However, despite this investment, outcomes are poor, with the United Nations Office on Drugs and Crime estimating that less than 1% of global illicit financial flows are recovered annually. To compound matters, crimes such as fraud are rising exponentially, meaning there is a stark imbalance between inputs from both the private and public sectors (in terms of time and investment in tackling financial crime), versus outcomes against criminals.

This imbalance is prompting stakeholders across the public and private sectors globally to question established ways of working and to consider how we can be both more efficient and effective in the fight against financial crime. A key challenge is that criminals – especially serious and organised criminals – do not operate in silos. Their criminal activities are international and the money they generate moves across borders and between institutions with ease. This cross-border, cross-institution activity is deliberate. Criminals are students of their chosen profession – they know that law enforcement and financial institutions do not, and cannot, collaborate at pace to stitch together, for example, a comprehensive view of global money flows, and they exploit that weakness to achieve their ends.

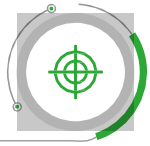
Enabling and accelerating collaboration between ecosystem stakeholders, including around intelligence and information sharing is therefore of critical importance if we are to break down silos and deliver better outcomes against criminals.

However, collaboration and information sharing will not flourish without the presence of some important enablers. These include trust, incentivisation, senior leadership, and perhaps most importantly of all, stakeholders require confidence in the legal basis for collaboration and information and intelligence sharing. These factors are discussed in more detail in a recent paper Deloitte has published alongside the Institute of International Finance[4].

For this reason, the European Union's (EU) latest Anti-Money Laundering (AML) package, and particularly Regulation (EU) 2024/1624[5], Chapter VI, Article 75, which seeks to enable innovation and enhancements in cross-sector and cross-border information and intelligence sharing through the creation of information sharing partnerships, is a hugely welcome and potentially significant step forward in the fight against financial crime.

This paper provides a high-level summary of Article 75 and the opportunities it presents.

2. Why was Article 75 created?



Over the last 10 years, stakeholders have demonstrated how public private information sharing partnerships (PPPs), such as the UK's Joint Money Laundering Intelligence Taskforce (JMLIT), can help stakeholders identify and tackle financial crime more effectively.

The value of PPPs has been recognised by the Financial Action Task Force (FATF) in publications such as *Partnership in the Fight against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*[6] and through the mutual evaluation process. It has also been noted by numerous commentators[7].

However, most PPPs remain small scale and often operate in addition to, or separately from, the Suspicious Activity / Transaction Reporting (SAR/STR) frameworks that have formed the cornerstone of information exchange between the regulated sectors and the National Financial Intelligence Units (FIU) for over 20 years.

In addition, almost all PPPs operate on a unilateral basis, with limited cross-border cooperation between PPPs, which undermines their ability to track criminal activity and money flows cross border. In the case of the SAR regime, there are mechanisms to share data cross border which are provided through the Egmont network; however, this exchange can take time, and its value can be reduced if intelligence is heavily redacted before it is shared.

Critically, neither PPPs nor SAR frameworks enable information to be shared directly between banks, instead requiring a central body (the PPP coordinator or the FIU) to coordinate. This can create a choke point that can slow down information exchange or undermine its collective analysis.

Article 75 is a powerful first step in addressing these challenges as it enables direct collaboration between banks, cross-border collaboration, and potentially brings together the best elements of both PPP and the SAR regimes. Proactive use of Article 75 should help both public and private sector stakeholders to improve the effectiveness of the AML framework at both the national and bloc wide level.

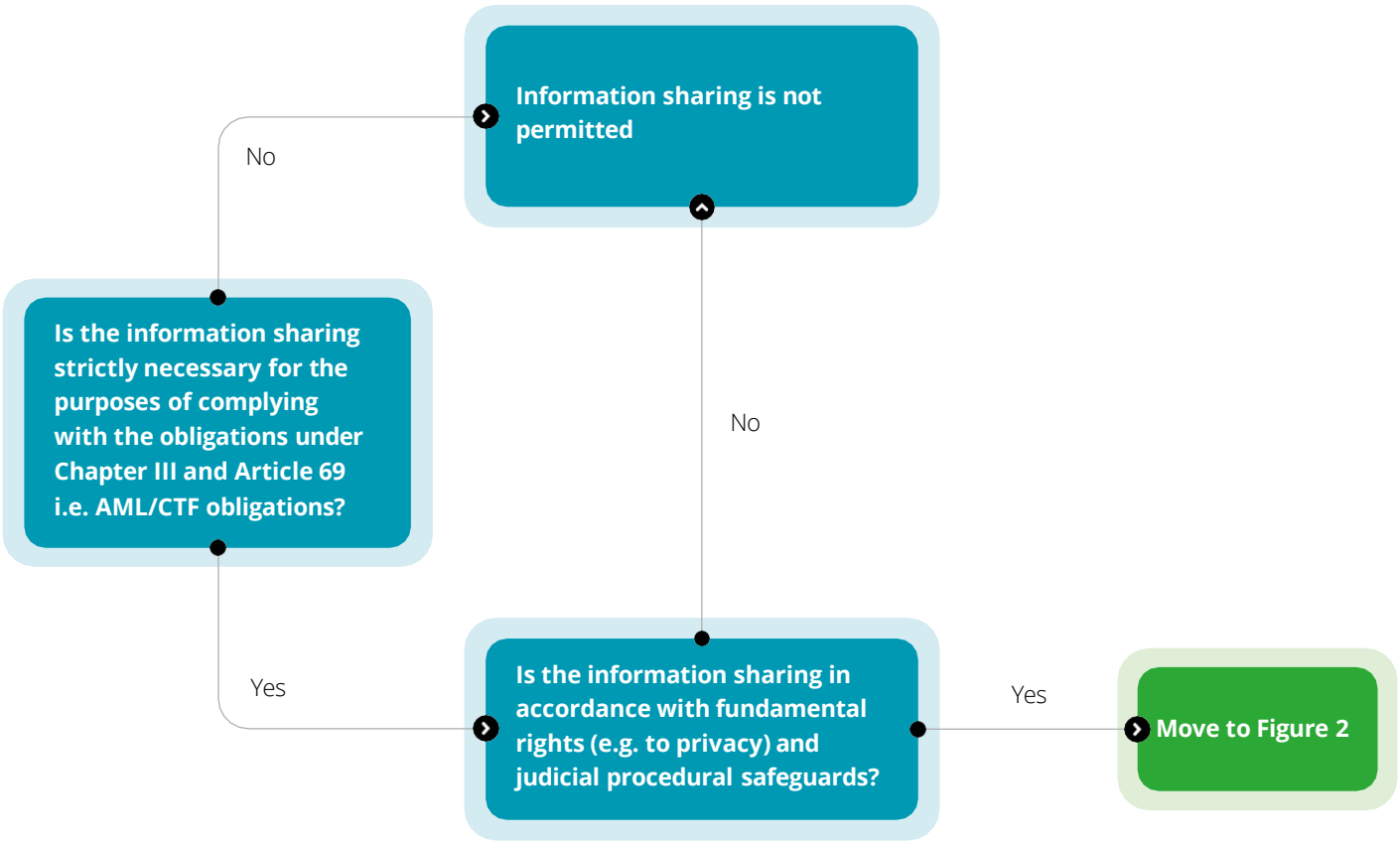
3. Article 75: an overview

Article 75 allows EU member states to create partnerships for the purposes of exchanging information to prevent money laundering (ML) and terrorist financing (TF) activity. The problem Article 75 is intended to address is clear, with the EU noting that "The exchange of information among obliged entities or between obliged entities and competent authorities can increase the possibility of detecting money laundering or terrorism financing taking place across more than one service provider."[8]

3.1. Who can share information under Article 75? Partnerships for information sharing can include participants from public and private sectors with regulatory responsibilities for preventing ML/TF. This can include obliged entities, FIUs in any EU country, and competent authorities such as supervisory authorities. Interestingly, the entire suite of obliged entities is included, which brings into scope lawyers, accountants, estate agents, casinos, and more. These sectors could provide highly useful additional insight into suspicious high-risk transactions in the context of information sharing partnerships.

3.2. When can information be shared? Information can be shared when necessary for the purposes of participants' performance of their tasks under relevant EU or national law related to preventing ML/TF. The precise focus of information sharing partnerships may vary, for example they could focus on developing a shared understanding of particular strategic threats or particular criminal networks. Figure 1 shows how this could work in practice.

Figure 1: An outline of when information can be shared under Article 75

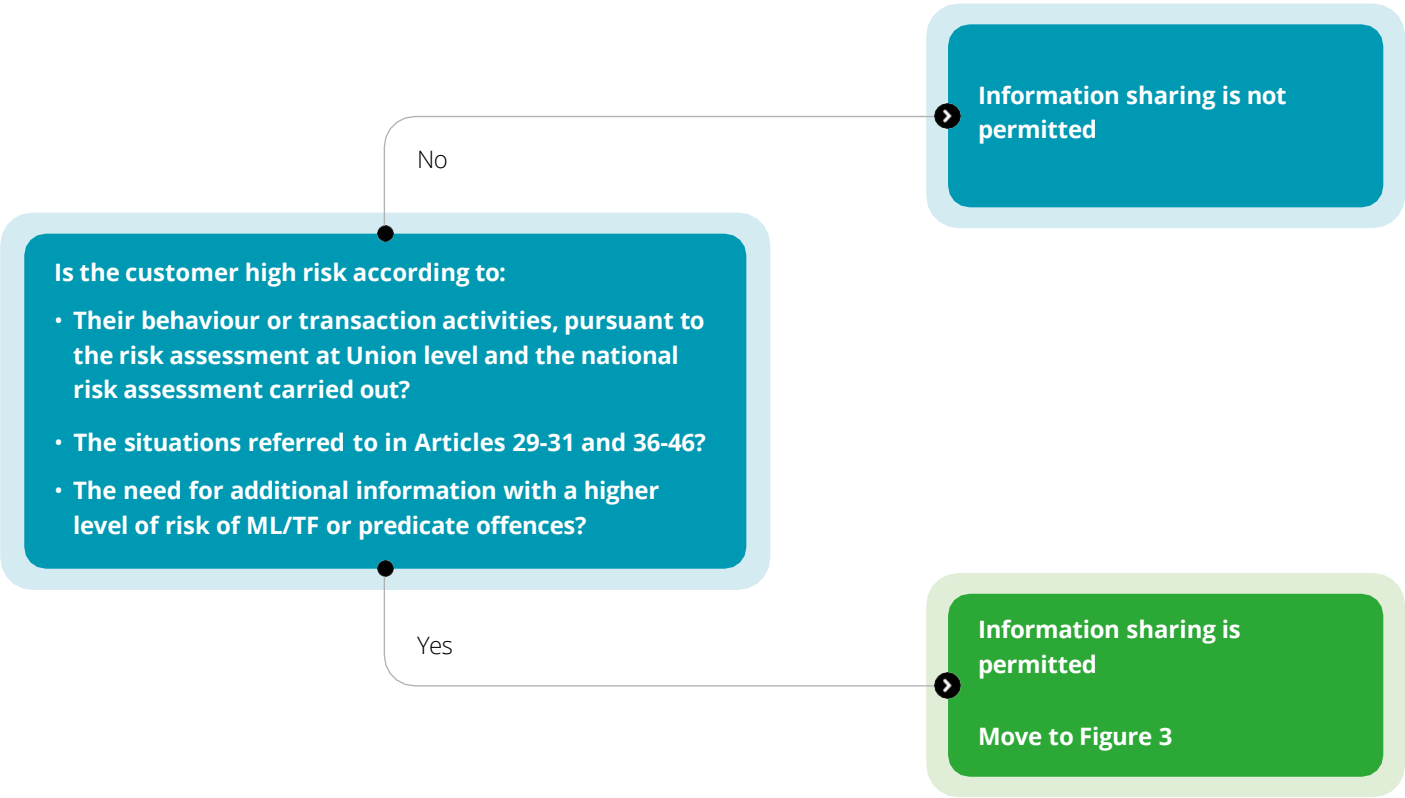


3.3. What information can be shared? Article 75(3) sets out the full range of data that can be shared. The scope is broad and includes operational information (e.g., information on customer transactions), personal data (e.g., customer names), information obtained through customer due diligence processes, and any information on suspicions in line with FIU suspicious reporting expectations as set out in Article 69.

However, data can only be shared where there are appropriate safeguards in place, and where it relates to high-risk customers, as set out in figure 2 below. Article 76 sets out additional safeguards around the handling of personal data that obliged entities might share for the purposes of preventing ML/TF, requiring for example, that it originates from reliable sources, and is compliant with wider EU rules to ensure it is up to date and accurate.

3.4. How can information be used? As set out in Article 75(4), obliged entities must record all instances of information sharing within the partnership and participants cannot rely solely on the shared information to comply with regulatory requirements. This means that recipients of information via partnerships must consider and assess the information received and carry out their own assessments of transactions involving the customer in line with their broader policies and procedures and the application of a risk-based approach. Information received should not be further transmitted, except in certain circumstances, such as when included in a report submitted to the FIU, provided to the AMLA, or requested by law enforcement or judicial authorities.

Figure 2: Criteria for information sharing under Article 75



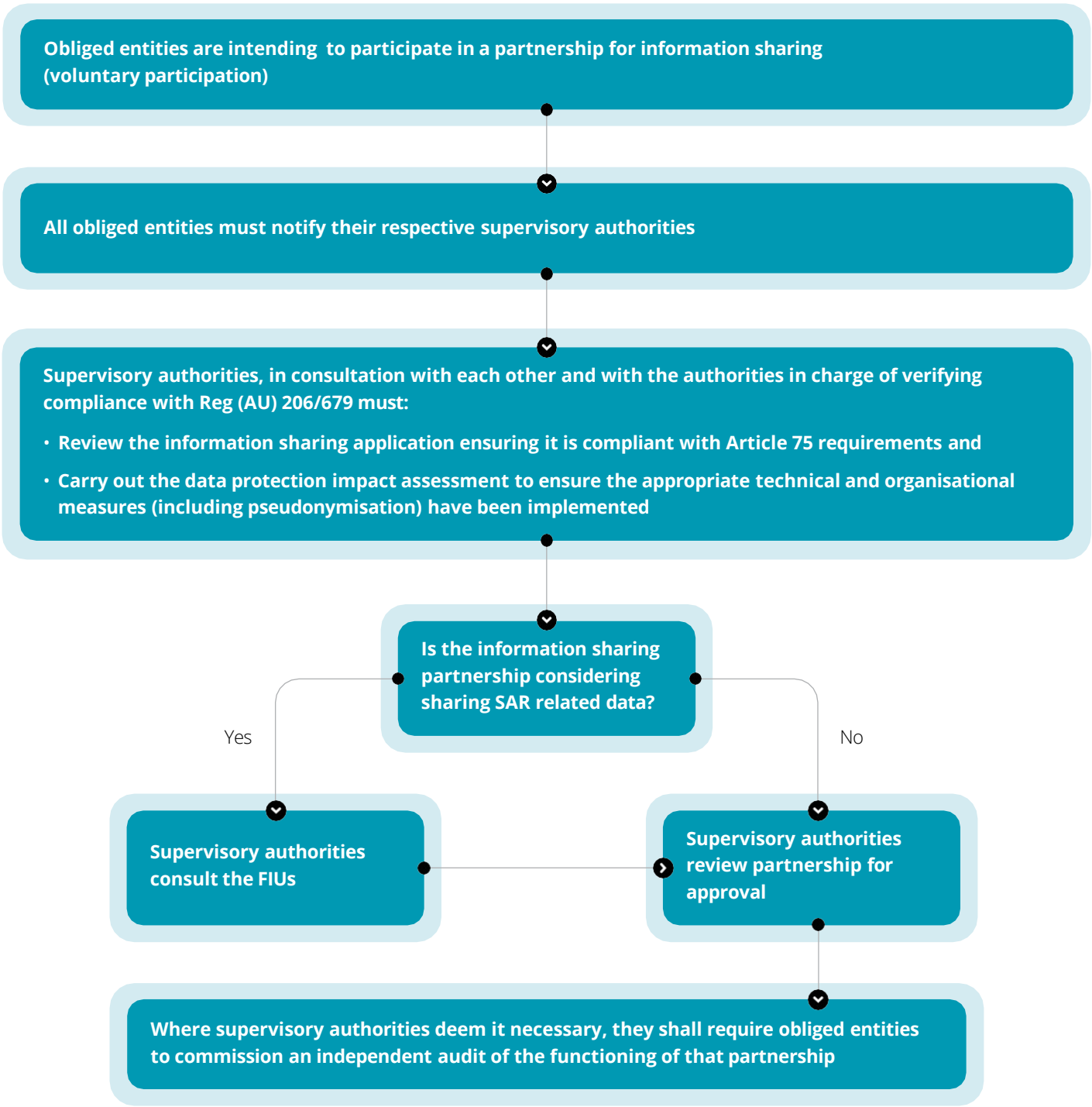
What information can be shared?
- Post suspicion SAR reporting (if approved by the FIU)
- Information on the customer and beneficial owner
- Purpose and intended nature and source of wealth
- Customer transactions
- Risk factors associated with the customer, including obliged entity's analysis of the risks associated with the customer

Note: Information generated through the use of AI, Machine Learning (ML) technologies, or algorithms may only be shared where these processes have been subject to adequate human oversight

4. Establishing a partnership for information sharing under Article 75

Figure 3 below is a high-level visualisation of our understanding of the process a partnership will need to go through before information sharing can take place.

Figure 3: A Deloitte view of the process for establishing an information partnership under Article 75



1. What additional factors must be considered?

- **Governance:** Article 75(4)(e) requires the partnership to set up and maintain appropriate governance and security processes, including recording all instances of information exchange.
- **Data privacy:** EU data privacy rules must be adhered to. For example, partnerships must conduct a Data Protection Impact Assessment (DPIA) prior to the processing of personal data in the context of an information sharing partnership. The DPIA can be completed and maintained on behalf of an ongoing partnership. Whilst it requires clarification, in our initial assessment, the DPIA does not need to be repeated every time information is exchanged, but rather can be completed once (and then maintained), on behalf of the partnership, providing the purpose of the partnership remains the same.
- **Supervisory oversight:** Partnerships must be approved by the supervisor of obliged entities seeking to collaborate in a partnership. The obliged entities' supervisor, as competent authority, must approve the DPIA and liaise with the FIU where appropriate. Supervisors can also commission an independent audit of partnerships where they deem it necessary. Where entities with different supervisors (e.g., a bank and an accountancy firm) form a partnership, we anticipate that both supervisors will need to approve the DPIA. This may require new forms of collaboration between supervisors too.
- **Obliged entities:** Obliged entities participating in information sharing are required to define policies and procedures for the sharing of information within their internal financial crime policy framework. These policies should determine the extent of information to be shared, describe the roles and responsibilities of the parties, and identify the risk assessments to determine situations of higher risk. This will require updates to existing frameworks.

5. The potential value of Article 75

Article 75 provides a unique opportunity to expand our understanding of emerging risks, develop cross-border collaboration and to disrupt financial crime at greater pace and scale.

5.1. Increased disruption of financial crime: By enabling increased information sharing between stakeholders and across borders, Article 75 will allow criminal networks and money flows to be identified and disrupted more effectively and more quickly. This could drive operational results, enable more criminal assets to be traced, restrained, and recovered, and should lead to better outcomes for the victims of crime.

It will also help stakeholders to develop a more precise and actionable shared understanding of key threats and risks, which will improve the focus and quality of reporting, and will inform the development of key financial crime processes (such as transaction monitoring). This will enable those processes to become more efficient and effective, helping to ensure better use is made of the capacity and capabilities that exist across the ecosystem.

5.2. Increased appetite to engage: The policy intent behind Article 75 is clear: stakeholders are being encouraged to collaborate in the fight against financial crime. It is hoped that this clear steer, supported by the new legal gateway will encourage financial institutions to participate.

This will not be without challenge. We know from other information sharing pilots that building new ways of working takes courage and leadership, and a willingness to work together to overcome a spectrum of practical challenges from data standards to the navigating of competition law. However, the development of PPP, as well as other innovations, such as the UK's recent pilot to share information between banks using GDPR, show that such challenges can be overcome, and that the opportunity to improve outcomes means they should be.

5.3. Better outcomes for obliged entities: Article 75 could help obliged entities to better manage their ML/TF risk by enabling them to build a more precise understanding of threats and to identify risk in their institutions that cannot be seen in isolation. This in turn will help enhance the application of the risk-based approach, enable the provision of more useful reporting to law enforcement, and help financial institutions reduce financial losses from fraud.

5.4. Progress made towards establishing trust: We know from other PPPs that building trust between stakeholders is key to building a more effective framework. This is considered in detail in our white paper *The effectiveness of financial crime risk management reform and next steps on a global basis*[9]. By providing a robust gateway, the EU is creating a strong foundation for partnership. We anticipate that this will enable the building of trust and mutual understanding between stakeholders over time, which is a key condition of a more effective financial crime framework.

In addition, by including all obliged entities within scope, Article 75 provides a good opportunity for non-financial sectors to build a more collaborative working relationships with FIUs and the broader private sector, which is not common at present. Also, the participation of the non-financial sector provides a unique opportunity to tackle criminal threats collectively and to understand how they operate from a diverse range of perspectives.

6. Does Article 75 go far enough?

It has been noted by a commentator that Article 75 does not introduce bold innovation[10], which could limit its effectiveness. Potential limitations noted include the fact that information can only be shared post suspicion or for high-risk customers, which could limit the gateway's powers to drive crime prevention. In this section, we explore some of the challenges that may arise linked to interpretation and complexity, compliance with wider legislative frameworks, and capacity. We also set out some of the lessons to be learned from the development of other information sharing partnerships.

6.1. Interpretation and complexity: Elements of Article 75 require interpretation. This includes the definition of key terms such as *high-risk customers*, as well as important parts of the process, for example, when a supervisor may deem it *necessary* to commission an independent audit of a partnership.

Additional guidance would provide useful clarity to participants, and this would in turn increase their willingness to engage in what is a voluntary process that does involve risk as it relates to the sharing of personal data in greater volumes than have previously been the norm.

In addition, Article 75 is, arguably, procedurally complex and novel. For example, it requires participants to secure advance approval to collaborate from supervisors, the completion of shared DPIA documentation, the agreement of data standards, and the use of pseudonymisation, etc. These elements and others could delay or complicate implementation if there is not clear guidance and it will require dedicated focus and commitment from partnership members to navigate through them.

Finally, while Article 75 clearly aspires towards cross-border sharing, this is a new area with a high degree of inherent complexity. Achieving cross-border sharing will for example, require consensus to be reached between different privacy regulators and the navigation of challenges around issues such as data localisation. Article 75 notes that "Responsibility for compliance with requirements under Union or national law shall remain within the participants in the partnership for information sharing", however there is not yet guidance as to how key challenges should be tackled. As in other areas, developing this guidance and best practice will take genuine leadership from partnership members.

6.2. Compliance with wider legislative frameworks: Partnerships must comply with strict rules that aim to protect fundamental rights including the right to privacy and data protection. There is a risk that fear of infringing these rules could deter participation in Article 75 partnerships given the regulatory risk created for obliged entities. Clear guidance and sharing of best practice will be key, but policymakers and supervisors should also consider how they can support innovation, for example, by providing clear support for the development and use of Article 75 partnerships, and perhaps even the development of some kind of regulatory recognition for participating in a high value but voluntary activity.

6.3. Capacity: Article 75 will require the new processes to be developed between institutions and within institutions to manage data privacy and financial crime regulatory obligations. This will take input from people who already have *day jobs*. Our experience of information sharing initiatives is that a dedicated secretariat or project management function is needed to ensure progress is maintained and that obligations (e.g., to different supervisors) are being effectively met.

6.4. Lessons Learned from the development of other information sharing partnerships: From practical experience and independent research, we have identified a number of key factors that are required for any kind of innovative information sharing partnership to flourish. These have been set out in figure 4 below.

Figure 4: Key enablers of success in the development of information sharing partnerships

Category	Success factor	Overview
Purpose	**Stakeholder engagement and leadership**	Identifying the right stakeholders and engaging with them as early as possible
	Common aims	Generating a common understanding of the aims and use cases to be met by the partnership
	Measures of success	Defining measurable outcomes to track partnership development
	Trusted relationships	Participating organisations trust each other and the quality of information shared with them
Design and delivery	**Process**	Reaching agreement between participants that they will apply the same process
	Data	Agreeing clearly defined data fields with common standards and agreed sharing criteria
	Technology enablers	Adopting the right technology to support automation and an easy approach to integration
	Organisational & Commercial model	Agreeing and implementing an appropriate structural model to implement and run the partnership
Risk mitigation	**Information security and data privacy**	Establishing data controllers and processors to own measures to protect sensitive information
	Legal framework	Establishing an appropriate framework to protect participants from regulatory action

7. Conclusion

The EU's assessment of the success of the implemented measures will be communicated in 2030. Before then, it is crucial that potential participants in Article 75 partnerships engage with the agenda for two reasons.

Firstly, Article 75 provides a unique opportunity for stakeholders to improve the efficiency and effectiveness of the collective response to financial crime. This clearly has merit in and of itself but is also critical in providing evidence to policy makers about the value of this approach, which will in turn encourage and enable further innovation in information sharing.

Secondly, stakeholders who engage practically with Article 75 will identify challenges and issues (for example, in relation to the provision or clarification of guidance) that can be fed back to policymakers as part of a virtuous circle of testing and improvement.

Remember, many stakeholders have been arguing for a long time to make the case for provisions that allow collaboration and information sharing to fight financial crime. When policy makers listen and respond, as they have with Article 75, they have played their part. The ball is now back in the court of the regulated sector and the FIUs. It is critical that we all do our best to play our part.

Contacts

Rasmus Grejs Beyer
Partner
Financial Crime Advisory
+45 24 94 59 22
rbeyer@deloitte.dk

Maria Damborg Hald
Partner
Technology & Transformation
+45 42 94 28 26
mahald@deloitte.dk

Andrew Robinson
Partner
Forensic UK
+44 [0] 20 7007 0613
andrewrobinson@deloitte.co.uk

Pernille Lassen
Director
Financial Crime Advisory
+45 30 93 61 76
plassen@deloitte.dk

Endnotes

1. Nasdaq Verafin 2024 Global Financial Crime Report | Nasdaq
2. Illicit Financial Flows | United Nations
3. Forrester Research True Cost of Compliance | LexisNexis Risk Solutions
4. Global financial crime prevention, detection and mitigation (deloitte.com)
5. Regulation - EU - 2024/1624 - EN - EUR-Lex (europa.eu)
6. Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing (fatf-gafi.org)
7. The Global Coalition To Fight Financial Crime Publishes Effectiveness Expert Working Group Position Paper – The Global Coalition to Fight Financial Crime (gcffc.org)
8. Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) (europa.eu)
9. The Effectiveness of Financial Crime Risk Management Reform and Next Steps on a Global Basis (deloitte.com)
10. EU Article 75 - Pan EU information sharing is coming, but will it be enough? - Financial Crime News (thefinancialcrimenews.com)

Deloitte.