Council of the European Union

Brussels, 23 November 2022
(OR. en)

15170/22

EF 346
ECOFIN 1223
DROIPEN 151
ENFOPOL 589
CT 205
FISC 231
COTER 283

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2022) 347 final
Subject:	COMMISSION STAFF WORKING DOCUMENT On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing

Delegations will find attached document SWD(2022) 347 final.

Encl.: SWD(2022) 347 final

EUROPEAN
COMMISSION

Brussels, 27.10.2022
SWD(2022) 347 final

COMMISSION STAFF WORKING DOCUMENT

On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing

1. Introduction

The Commission's *Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*[1] emphasised the importance of the effective exchange of information in the fight against money laundering and terrorist financing (ML/TF). The action plan stressed that in the context of making better use of financial intelligence, the roles of public-private partnerships should be encouraged to the extent possible as the sensitive nature of the information might limit its sharing. In the Action Plan, the Commission committed to issue guidance on public-private partnerships, which is presented in this document.

The Commission staff working document provides a number of examples of public-private partnerships in the domain of anti-money laundering and countering the financing of terrorism (AML/CFT) that have been initiated in EU Member States. These cases point at their flourishing across the EU, which entails both opportunities and legal considerations. This non-binding document does not aim to harmonise the concept of public-private partnerships. Instead, it examines the way in which such partnerships function within the EU. The aim is to improve the general understanding of public authorities, the private sector and all relevant stakeholders of the main features and the associated opportunities, specific legal considerations as well as observed best practices, thereby encouraging the role of public-private partnerships in the fight against ML/TF. Section 4 presents examples of public-private partnerships in the Union, while Sections 5 and 6 outline the opportunities and relevant legal frameworks. Finally, Section 7 identifies a number of best practices.

The document does not cover the exchange of information between private entities ('private-to-private' exchanges). This is regulated by the provisions contained in Article 39 of the Anti-money Laundering Directive[2]. Neither does the document cover an assessment of personal data protection aspects, as the European Data Protection Board is the competent body to issue guidance on these issues at the EU level.

2. What is a 'public-private partnership in the framework of preventing and fighting money laundering and terrorist financing'?

The role of Financial Intelligence Units (FIUs) and private sector obliged entities within an AML/CFT preventive framework requires information to be shared in specific circumstances. Within the private sector, obliged entities such as credit and financial institutions and providers of gambling services, conduct due diligence on their customers, including

[1] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (2020/C 164/06), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0513%2803%29.

[2] 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 (Text with EEA relevance), OJ L 141, 5.6.2015, p. 73–117 as amended by Directive (EU) 2018/843.

transaction monitoring. They have an obligation to submit to the FIU reports on suspicious transactions and activities (STRs/SARs) where they know, suspect or have reasonable grounds to suspect that funds are the proceeds of crime or are related to terrorist financing. Obliged entities are required to respond to all requests for information from FIUs[3].

To prevent and combat ML/TF, FIUs are tasked to collect and analyse information they receive and other information they can access, with the aim of establishing links between suspicious transactions and underlying criminal activity. Where FIUs suspect money laundering, its predicate offences or terrorist financing, the results of their analyses are disseminated to law enforcement authorities[4]. Law enforcement bodies use FIUs' analytical reports in their investigative work. In addition, law enforcement authorities can, subject to national procedural rules, request information from obliged entities in the framework of a criminal investigation.

Public-private partnerships are generally understood to imply the set-up of a specific framework for sharing information between FIUs, law enforcement authorities and the private sector. Within such partnerships, information need not necessarily flow in the manner and order set out above, as some partnerships may enable the exchange of information from obliged entities to law enforcement authorities and vice-versa. However, there is no commonly agreed definition of what constitutes a public-private partnership in the framework of preventing and fighting ML/TF.[5]

Over recent years, the Commission has supported projects under the Internal Security Fund on public-private partnerships and the sharing of information[6]. Various models of public-private partnerships have been set up across the EU over the course of the past years. These partnerships may vary in terms of structure, objectives, participants and the type of information exchanged. However, public-private partnerships that involve the sharing of information between law enforcement authorities, FIUs and the private sector are set up for two main reasons:

---

[3] Article 33 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

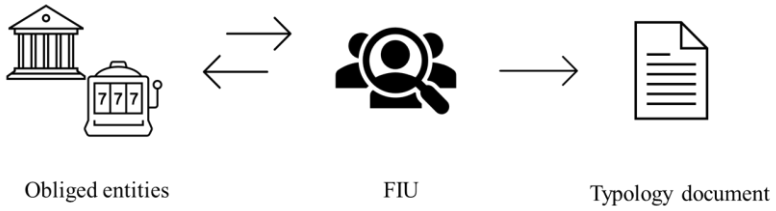
[4] Article 32 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[5] An occasional paper by the Future of Financial Intelligence Sharing (FFIS) programme of the Royal United Services Institute (RUSI) uses the term 'financial information-sharing partnerships', which could entail sharing of operational intelligence to enhance ongoing investigations' and 'collaborative working to build understanding of threats and risks'. Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', Occasional Papers, 17 October 2017, RUSI https://rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime. For further reading, Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme, *'Five years of growth in public-private financial information-sharing partnerships to tackle crime'*, available at: https://www.gcffc.org/wp-content/uploads/2020/08/FFIS-Report-Five-Years-of-Growth-of-Public-Private-Partnerships-to-Fight-Financial-Crime-18-Aug-2020.pdf.

[6] To be noted that the Commission could also provide technical support to Member States under Regulation (EU) 2021/240 of the European Parliament and of the Council of 10 February 2021 to promote reforms aimed at reinforcement of the fight against money laundering.

- to exchange strategic information (e.g. typologies, trends, risk indicators, feedback on suspicious transaction and activity reports) between FIUs and obliged entities;
- to exchange operational information between public authorities and obliged entities on 'persons of interest' for law enforcement.

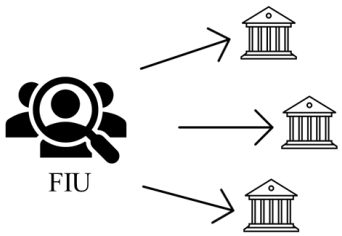
In practice, some public-private partnerships may enable information exchange on the two



An example of a partnership in which obliged entities and the FIU exchange strategic information on emerging risks and red flags noted in the course of their respective operations. This demonstrates a two-way flow of information that results in the development of typologies and other educational materials. Documents may then be distributed, for instance among public authorities or obliged entities.

Source: Commission services

levels, i.e. strategic and operational information.



An example of a strategic exchange in which the FIU shares a set of sector-specific risk indicators to a group of similar obliged entities. These are then used by the obliged entities to calibrate their transaction monitoring systems and detect more or newer suspicious activities relating to a given emerging trend.

Source: Commission services

Section 4 of this document note examines in greater detail different levels of information exchange through public-private partnerships, their set-up and objectives.

3. Consultation activities

Since the adoption of the action plan, the Commission services have carried out consultation activities linked to the setting-up and operation of public-private partnerships in the field of fighting ML/TF with stakeholders from the private sector, Member States, EU agencies and bodies, academic organisations, research institutions, non-governmental organisations (NGOs) and the general public. As outlined in the Commission's consultation strategy[7], the consultation activities aimed to collect relevant evidence in the form of views and opinions supported by facts and figures on various aspects relating to public-private partnerships.

An open public consultation ran from July 2021 to November 2021[8]. The Commission received 38 contributions. Of these, 13% were individual responses from EU citizens. In addition, a wide range of stakeholders provided replies, including business associations (24%), companies or business organisations (21%) (mainly within the banking sector), public authorities, including Europol (13%), NGOs (8%), academic/research institutions (5%) and trade unions (3%).

Furthermore, recognising FIUs as important stakeholders in the context of public-private partnerships, the Commission's services circulated a questionnaire among members and observers of the EU FIUs' Platform – an expert group of the Commission. 14 FIUs replied to the questionnaire. Europol, an observer in the expert group, submitted a position paper based on its experience with the Europol Financial Intelligence Public-Private Partnership (EFIPPP).

All input and evidence received fed into the preparation of this document. The synopsis report of the consultation activities[9] summarises the information submitted.

4. Types, objectives and set-up of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing

As set out in Section 2 above, public-private partnerships for information exchange between law enforcement authorities, FIUs and the private sector mainly concern the exchange of two different types of information, namely strategic or operational information. Strategic information refers to typologies, trends, risk indicators and general feedback on suspicious transaction reports, and does not usually include information on specific cases, persons or transactions. Operational information relates to specific cases and would include data on known persons and transactions. The following sections provide more information on the two types of exchanges.

[7] Consultation strategy: Guidance on the rules applicable to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing, available at: Consultation strategy: Commission guidance on the rules applicable to the use of public private partnerships in the framework of preventing and fighting money laundering and terrorist financing (europa.eu).

[8] For more information, Preventing money laundering and terrorist financing – EU rules on public-private partnerships (PPPs) (europa.eu).

[9] For further information on the consultation activities, please look at the Annex to this document.

The case studies outlined in this section describe some of the public-private partnerships established within Member States[10].

a. Public-private partnerships for the exchange of strategic information in the framework of preventing and fighting ML/TF, their objectives and set-up

i. Exchange of information on ML/TF typologies, patterns, trends and risk indicators

The majority of public-private partnerships set up in the EU bring together public authorities (FIUs, AML/CFT supervisors and law enforcement authorities) and private sector entities.[11] They exchange strategic information on patterns, trends, and typologies on criminal behaviour and ML/TF methods, and they develop ML/TF red flags and risk indicators. Such exchanges aim to increase a jurisdiction's understanding of ML/TF risks and threats and to enable obliged entities to calibrate their detection systems to more effectively detect money laundering, its predicate offences and terrorist financing.

Case study - German Anti-Financial Crime Alliance[12]

In September 2019, the German FIU, the Federal Financial Supervisory Authority (BaFin) and the Federal Criminal Police (Bundeskriminalamt) together with representatives of 15 German banks established the 'Anti-Financial Crime Alliance (AFCA). In total, AFCA consists of 36 members, including 19 financial institutions, 7 entities from the non-financial sector, 2 non-obliged entities and 8 public sector authorities. AFCA's objective is to establish a permanent platform for the exchange of strategic information and for cooperation in the fight against money laundering and terrorist financing in Germany.

AFCA's governance consists of four bodies: a board, a management office, an expert group and working groups. The latter form the operational heart of AFCA. Working groups facilitate the regular sharing of information on subject-related developments, phenomena-related cases and topics that might affect the suspicion reporting system and obliged entities' detection systems.

Source: FIU Germany, June 2021.

In some cases, the established public-private partnerships are 'sector-specific', covering a particular group of obliged entities.

Case study - Austrian public-private partnership

In Austria, two public-private partnerships have been established:

[10] Such partnerships are not endorsed by the Commission and are presented for informative purposes only. Any reference to these cases does not imply any assessment of their compatibility with EU law.

[11] These usually include the private sector entities that are obliged to apply specific measures in order to prevent ML/TF. The measures include conducting 'customer due diligence' (CDD) and reporting of suspicious transactions and activities to their national FIU.

[12] Further information available on BaFin - News - BaFin enters into public-private partnership with other public … and on Zoll online - Anti Financial Crime Alliance.

Partnership with the financial sector: the Financial Crime working group was set up by the Federal Ministry of Finance in autumn 2019. In 2021, the Austrian FIU took over the management of the working group and is now chairing meetings, together with the Federal Ministry of Finance, while also being responsible for the thematic orientation of the partnership. The working group is a forum for cooperation between the FIU and the private sector, enabling the exchange of current trends and phenomena in the field of anti-money laundering and on technical challenges in the operational exchange of information. Members of the working group are the Financial Market Authority, leading Austrian credit and financial institutions, money remitters, virtual asset service providers and insurance companies and financial service providers. The main objectives of the working group include: i) improving transaction monitoring of credit and financial institutions based on the experience of participants represented in the working group; ii) standardising the transmission of STRs via goAML using XML[13]; and iii) providing effective feedback from the FIU to obliged entities.

Partnership on betting and gambling: the working group for a harmonised interpretation of state laws on betting and gambling. The working group is led by the Austrian FIU and its members include representatives of regional governments, the chamber of commerce, the Austrian association for sports betting, legal experts and Austrian betting companies. Its main objectives include: i) issuing guidance papers for the gambling and sports betting sectors, including on internal organisation and controls, due diligence and reporting obligations and risk analysis; and ii) issuing guidance on how to conduct risk-based oversight activities for competent authorities.

Source: FIU Austria, April 2022.

In other cases, the objectives of the public-private partnership go beyond the mere exchange of strategic information and cover a broader set of purposes. These include, for example, performing analyses, preparing guidelines and recommendations, proposing legislative initiatives to improve the national AML/CFT framework and organising training activities. Furthermore, the set-up of a particular public-private partnership may cater for participation by a wider array of public authorities.

Case study - Lithuanian Centre of Excellence in Anti-money Laundering[14]

The Centre of Excellence in Anti-money Laundering was established in 2021 by Lithuania's Ministry of Finance, the Bank of Lithuania, and eight commercial banks. Other financial market participants will be invited to join its activities in the future. The Prosecutor General's Office, the Financial Crime Investigation Service, the Special Investigation Service, the Police Department, the Ministry of the Interior, and the State Tax Inspectorate also take part in joint actions with the Centre.

As the AML Centre of Excellence evolves, it will expand its membership across the private sector, when other financial market participants (financial and non-financial market players) will be invited to join. The Centre combines the efforts of public and private sectors in strengthening the country's AML/CFT framework, by:

[13] goAML is a software system developed by the United Nations Office on Drugs and Crime for use by FIUs. XML (Extensible Markup Language) is a text-based format used to represent structured information.
[14] Further information available on: Centre of Excellence in Anti-Money Laundering | Bank of Lithuania (lb.lt).

a) ensuring high-level collaboration and information sharing targeted at combating financial crime; and

b) raising public awareness and building knowledge through sector-wide comprehensive educational programmes aimed at improving public and private sectors' capabilities to detect and disrupt financial crime.

The AML Centre of Excellence has formed task force groups that bring together government, law enforcement and financial industry partners focused on protecting both Lithuanian citizens and the financial system from being exploited by means of money laundering and terrorist financing.

Source: FIU Lithuania, April 2022

Another such example is the Belgian public-private partnership, which - in addition to the exchange of strategic information on typologies, trends, and patterns - also provides a forum for the discussion of issues related to the implementation of AML/CFT rules by banks and insurance companies and for the exchange of views on new pieces of legislation.

Case study - Belgian public-private partnership

The Belgian public-private partnership initiative was set up in 2021. It includes the Ministry of Finance – Treasury (as head of the platform), the CTIF-CFI (Belgian FIU), the Belgian National Bank (supervisor of banks and insurance companies), the FSMA (supervisor of insurance brokers and exchange offices), Febelfin (representing banks and many other financial institutions), Pay Belgium (representing payment service providers), and Assuralia (representing insurance companies).

The objectives of the partnership include: i) sharing information on typologies, trends, patterns, mechanisms and new ML/TF threats and risks; ii) sharing the results of specific strategic analysis made by the FIU or by the financial sector; iii) providing a secure IT tool to share specific confidential documents on typologies, mechanisms or new threats; iv) discussing issues related to the implementation of AML/CFT law by banks and insurance companies; v) exchanging views on new legislation and vi) studying how personal data could be exchanged in specific ML/TF cases or investigations, also in the context of the General Data Protection Regulation.

Source: FIU Belgium, April 2022

Some Member States have taken a different approach. Instead of setting up one main public-private partnership, they have established a number of smaller partnerships that focus on sector-specific trends and typologies.

Case study - Sector-specific public-private partnerships in Ireland

The first Irish public-private partnership – the Joint Intelligence Group - was set up in 2017. It consists of the five main banks in Ireland which submit approximately 60% of all STRs as well as Western Union Ireland. Another public-private partnership with representatives from Irish-based international banks was set up in 2020. This was followed in early 2021 by another partnership – the Joint Practices Group - with representatives from accountancy bodies. The fourth partnership, involving obliged entities from the fintech sector was established in May 2021 and also includes the Electronic Money Association.

The objectives of the public-private partnerships are the following: i) contribute to AML/CFT awareness and capability; ii) contribute to Ireland's resilience against serious and organised crime and iii) contribute to a responsive and agile AML/CFT framework. Strategic information is shared on current crime threats and AML/CFT trends and typologies. There is also a focus on how to improve the feedback to obliged entities and the quality of STRs/SARs they submit.

Source: FIU Ireland, June 2021

It is important to highlight that the EU has established a cross-border public-private partnership, namely Europol's Financial Intelligence Public-Private Partnership (EFIPPP).

Case study - Europol's Financial Intelligence Public-Private Partnership[15]

The EFIPPP is a transnational information sharing mechanism launched in 2017. Its members and observers include 29 competent authorities, 28 financial institutions, 5 national public-private partnerships and 19 other organisations, including international organisations, EU institutions, national regulatory authorities, think-tanks and academia.

EFIPPP's objective is to provide an operationally focused environment for cooperation and information exchange between Europol, law enforcement authorities, FIUs and other competent authorities, and financial institutions. Some of the EFIPPP activities include the exchange of strategic intelligence and expertise, the development of analytical products and the development of crime typologies presenting red flags and risk indicators on key predicate offences and *modi operandi* for money laundering and terrorist financing.

Source: EFIPPP, April 2022.

ii. Provision of feedback on the quality of STRs/SARs

Some Member States have set up public-private partnerships with the objective to provide feedback to obliged entities in order to improve the quality of the suspicion reporting system. The currently applicable legal framework requires Member States to ensure, where practicable, that FIUs provide to obliged entities timely feedback on the effectiveness of, and follow-up to reports of suspected money laundering or terrorist financing[16]. Public-private partnerships are not required as such under the AML/CFT framework; they have rather

[15] The objectives of EFIPPP include:

- supporting national public-private partnerships, thereby also operating as a network
- developing shared intelligence images and understanding threats and risks
- facilitating tactical and operational information sharing
- exploring new possibilities in sharing information
- supporting, coordinating and initiating international actions
- promoting the use of new tools and technology.

Further information available on: European Financial and Economic Crime Centre - EFECC | Europol (europa.eu).

[16] Article 46, paragraph 3 of the 5th Anti-money Laundering Directive. This provision requires Member States to ensure, where practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided to obliged entities.

developed in some Member States in order to complement it and ensure the flow of information amongst the relevant actors.

Case study – Malta's Financial Intelligence Analysis Unit's (FIAU) feedback system[17]

The provision of feedback on STRs/SARs is one of the main pillars of Malta's FIAU public-private partnership programme. FIAU has put in place a feedback mechanism, whereby it informs obliged entities whether STRs/SARs contain the necessary information and, if not, what additional information should have been included in the report.

The ultimate objective of this feedback mechanism is to enable obliged entities to improve the quality of their suspicious transaction reports. This would then allow FIAU to reach a quicker determination about whether or not the STR/SAR contains indications of ML/TF or other illicit activities.

From a more operational perspective, FIAU also provides feedback at the end of the analytical process, whereby obliged entities are given high-level feedback on FIAU's outcome following their submission.[18]

Source: FIAU Malta, June 2021

The type of feedback that can be provided includes the following.

- Feedback on the quality of a single report, for example, indicating whether a report is complete or lacks information and/or documents, whether a suspicion is clearly described, or whether the obliged entity overlooked any relevant indicators.
- General feedback on quality of reports submitted by an entire sector.
- Whether the obliged entity has missed certain red flags and/or certain ML/TF risks associated with its products and services.
- Whether there are known *modi operandi* and typologies that the obliged entity has overlooked.
- Statistical data on the number of reports submitted per sector across a number of years. Such data may be useful for comparing sectors, for comparing increases (or decreases) in reporting by a sector over time, and for individual entities to understand how they are performing in comparison with their peers.
- Statistical data on the number of disseminations resulting from reports, across a number of years. Such data is useful for understanding whether there is an improvement in the quality and usefulness of reports.

FIUs may consider targeting the various types of feedback to individual entities to groups of entities bearing similar features (for example, entities of the same size, entities providing similar services or targeting similar types of customers) or to an entire sector or to all obliged entities in the respective jurisdiction.

[17] Further information available on: Public-Private Partnership - FIAU Malta.
[18] Section 4.b ii of this document includes more detail on the provision of operational feedback following an analysis.

The frequency of feedback may vary depending on the type and recipient, for instance:

- in some cases, FIUs may be in a position to provide feedback on individual STRs/SARs;
- periodically to individual entities (e.g. high reporting entities);
- periodically to a sector;
- annually to all sectors.

Various channels may be used for providing feedback, including the usual reporting channels, sectoral documents or annual reports.

FIUs may also consider providing qualitative and quantitative feedback during outreach initiatives, training events and conferences, or holding meetings with sectors or representative bodies specifically for this purpose.

b. Public-private partnerships for the exchange of operational information in the framework of preventing and fighting ML/TF, their objectives and set-up

i. Objectives of the exchange of operational information

Operational public-private partnerships are arrangements between the private sector (including obliged entities), FIUs and law enforcement authorities. These partnerships aim to enhance collaboration and to increase the effectiveness of national AML/CFT frameworks through the sharing of data, for example, operational information on specific persons, transactions and cases.

In the context of operational public-private partnerships presented in the case studies below, competent authorities share information, including sensitive information, with the private sector to trigger monitoring of the financial conduct of persons and entities of interest. This might also include the sharing of additional information that may be helpful in rendering the monitoring more effective (for example, information on contact persons or the business activities of the targeted person). Alternatively, competent authorities provide a private entity criminal intelligence, with the aim of allowing the private entity to search its data records in a targeted way. The sharing of such information takes place in accordance with national law.

Case study - Swedish Anti-Money Laundering Intelligence Task Force (SAMLIT)[19]

In June 2020, Sweden set up a pilot public-private partnership between the Police's intelligence unit at the National Operations Department, the Swedish Bankers' Association and five commercial banks. In 2021, Sweden decided to formalise the SAMLIT structure and planned for January 2023 the introduction of new legislation to facilitate the sharing of information.

[19] Further information available on: SAMLIT | SEB (sebgroup.com).

The SAMLIT organisation consists of: steering committee, delivery group (secretariat), operations committee, operational intelligence group; strategic intelligence group (expert working group) and legal working group.

The purpose of the partnership is to enable improved effectiveness in information sharing to support the detection, investigation and prevention of money laundering and terrorist financing. In addition to improving the collective understanding of the ML/TF threat and informing the banking sector of how to strengthen its systems and controls and to prioritise identified risks, SAMLIT aims at disrupting ML/TF activity by providing comprehensive financial information to law enforcement on specific cases.

Source: FIU Sweden, April 2022.

Case study - Dutch experience with public-private partnerships

FIU Netherlands has set up a number of public-private partnerships. One of them is the Fintell Alliance between the FIU and several obliged entities (in particular five major Dutch banks). The Fintell Alliance aims to enhance knowledge and insight that may lead to operational analyses, including through sharing of anonymised FIU analyses and direct exchanges between banks within the legal boundaries.

Besides the Fintell Alliance, the FIU also cooperates and exchanges information on a structural level through public-public partnerships or public-private partnerships, such as: (i) Financial Expertise Centre (FEC)[20], which is a public-public partnership, aiming to strengthen the integrity of the financial sector by promoting preventive and repressive measures; (ii) the FEC PPS[21] Serious Crime Task Force (SCTF)[22], which is a taskforce aiming at facilitating cooperation between partners for the prevention and detection of serious crime, in the interest of protecting the integrity of the financial sector, through the identification, investigation, and prosecution of essential financial facilitators and brokers that offer their services to organised crime groups; (iii) the TF PPS FEC project, better known as the FEC TF Task Force[23] set up in June 2017. Both task forces are FEC's public-private partnership initiatives. The TF Task Force was a pilot involving four public authorities (the Netherlands Police, the Public Prosecutor Office, the FIU-NL, and the Fiscal Information and Investigation Service) and six banks. In both task forces, cooperation focuses on the sharing of operational data regarding police data in the Counter-funding of terrorism and serious crime framework, leading to the reporting of unusual transactions to the FIU. Both have become permanent task forces.

Source: FIU Netherlands, May 2022

ii. The provision of feedback on impact and outcome of STRs/SARs

20 Home - FEC-partners

21 Publiek-private samenwerking.

22 Serious Crime Taskforce leidt tot structurele samenwerking | politie.nl

23 Samen effectief - FEC-partners

Operational public-private partnerships may also have as an objective the improvement of obliged entities' customer due diligence by providing feedback on the impact and outcome of STRs/SARs. In particular:

- competent authorities may provide obliged entities with information pertaining to specific STRs/SARs, for example through the provision of feedback on whether a transaction or customer mentioned in a particular STR/SAR is, according to the assessment of the authority, indeed linked to crime, or that there is reasonable suspicion to this effect;
- compliance-focused public-private data sharing may entail the provision of information independently of any particular SAR, with the aim of enabling the obliged entity to improve its risk detection capacity, for example providing profiles of relevant offender types or even information about particular suspects and their activities.

Case study - Finnish Anti-Money Laundering Intelligence Task Force

Finland has set up an AML Expert Working Group with the aim of providing practical implementation of AML obligations and to further improve the quality, content and processes of reporting on suspicious transactions. The AML Expert Working Group is composed of the Finnish FIU, which acts as chair of the group, the National Bureau of Investigation, and 16 private entities, i.e. 14 large and medium-sized banks, one gaming firm and one virtual asset service provider.

The objectives of the AML Expert Working Group are: (i) to enhance cooperation between the competent authorities and the private sector with a focus on contributing to the objectives of crime prevention; and (ii) to effectively prevent, detect and investigate money laundering, predicate offences and terrorist financing, and refer cases to criminal investigation by means of high-quality reporting on suspicious transactions.

In the framework of the AML Expert Working Group, its members exchange operational information, in compliance with current legislation, on suspicious transactions and targets specified in the Anti-Money Laundering Act. Moreover, to improve crime prevention processes, the AML Expert Working Group aims to: (i) remove obstacles to the exchange of information; (ii) exchange information on current *modi operandi* and money laundering risks; (iii) improve the capabilities of obliged entities to better identify suspicious transactions, for example by crime type; (iv) give feedback on the impact and outcomes of suspicious transaction reports and the successes made; and (v) propose how the prevention processes of the FIU and obliged entities can be improved.

Source: FIU Finland, May 2022

5. Opportunities and potential added value

Based on the input and evidence received, this document identifies a number of areas in which public-private partnerships for the exchange of information between law enforcement agencies, FIUs and the private sector could complement the current AML/CFT framework and bring added value.

i. Improve understanding of ML/TF risks and focus efforts in line with threats

Information from FIUs and law enforcement authorities on typologies, trends, red flags and risk indicators may enable obliged entities to improve risk assessments, customer due diligence processes, transaction monitoring and suspicion reporting. Criminals constantly adapt their activities and methods in order to exploit certain weaknesses in, for example, legislation, products and services. Sharing strategic information on risks allows FIUs and banks to develop more detailed risk typologies that can be used to improve awareness of new criminal techniques and emerging threats. This may lead to obliged entities detecting more potential criminal activities, submitting more targeted and better-quality STRs/SARs. As regards competent authorities, it may result in improving the quality of analyses and investigations by better focusing their resources where the real threats lie.

Moreover, strategic information sharing can support the proportionality of data processing. By developing clear risk typologies, public-private partnerships may help obliged entities to better understand the specific risks (and relevant indicators) associated with certain products, channels and customers, and ultimately to develop more refined internal policies and better customer due diligence. A better risk understanding may help reduce negative effects resulting from insufficiently detailed risk understanding, such as the unwarranted de-risking of categories of customers or the application of higher than necessary risk ratings.

ii. Improve the quality of STRs/SARs submitted by obliged entities

Stakeholders, including FIUs and obliged entities, highlight that public-private partnerships may bring added value when it comes to improving the quality, content and processes linked to the submission of STRs/SARs by obliged entities. The improvement results from the provision of feedback by the FIU, the sharing of ML/TF trends and typologies and participation in exchanges of operational information.

Feedback from FIUs to obliged entities can contribute to a better understanding of FIU's needs. It may also help obliged entities to produce more meaningful and useful reports that are of better quality. Improving the quality of STRs/SARs would also lead to reducing false positives and making sure that the national FIU is not overwhelmed with information that it struggles to process and which is of limited value for the fight against ML/TF. Moreover, post-STR/SAR feedback may also help to ensure that certain categories of customers do not permanently suffer the consequences of an erroneous risk assessment by the obliged entity.

iii. Build trust among public authorities (FIUs, law enforcement, supervisors) and obliged entities

Trust is the cornerstone of an effective cooperation and exchange of information. Public-private partnerships are fora where stakeholders can discuss in an informal setting the various issues regarding money laundering and terrorist financing. The collaborative nature of public-private partnerships may provide each party with a better understanding of how the other party operates, its functions, and the information it requires to carry out those functions appropriately. This may in turn improve cooperation between private entities and public sector bodies.

It is worth pointing out that building trust is both an opportunity and a challenge in the context of AML/CFT public-private partnerships. Many consulted stakeholders reported that building trust takes time and requires commitment from all partners involved.

iv. Enable a more targeted intelligence picture

Access to high-quality information is essential for law enforcement authorities to effectively investigate money laundering, its predicate offences and terrorist financing. A public-private partnership could enable law enforcement, in particular through the exchange of operational data, to cross-match financial and criminal information, and intelligence in order to create a more accurate and targeted intelligence picture. This could lead to more successful investigations and more effective law enforcement action with benefits across the entire follow-up process, including the prosecution and conviction of perpetrators and confiscation of illicitly obtained assets.

Overall, public-private partnerships have the potential to complement the continuous efforts to detect suspicious transactions and activities and develop financial intelligence to combat money laundering, its predicate offences and the financing of terrorism. Particularly with regard to countering the financing of terrorism, public-private partnerships can provide intelligence on persons of interest to obliged entities that allow them to better identify financial movements which are otherwise often difficult to distinguish from legitimate transactions.

6. Specific legal considerations

Exchange of information among partners entails a number of legal considerations, in particular as regards the handling of sensitive information, be it confidential information relating to financial analyses by FIUs and criminal investigations, or personal data. Therefore, this section focuses on legal considerations to be taken into account in the context of exchanges of information on specific persons, transactions and cases, which typically occur within partnerships set up for the exchange of operational information. However, considerations on the exchange of data within strategic partnerships, such as risks to data security, should not be neglected.

AML/CFT legislation currently in force already requires obliged entities to identify suspicious transactions and activities, to submit STRs/SARs to national FIUs and to respond to requests for information by national FIUs. The gathering of information from private parties by competent authorities in the framework of a criminal proceeding is already regulated by national criminal procedural rules. This is to safeguard the protection of the secrecy of law enforcement authorities' activities, the right to a fair trial and an effective remedy as well as the presumption of innocence, and the rights of defence to which each person is entitled in each phase of investigative and prosecutorial activities.

The exchange of information between public authorities and obliged entities in the context of public-private partnerships takes place in accordance with the existing national legal

framework, which aims to safeguard privacy and other fundamental rights[24]. A set of considerations are worth keeping in mind, as covered below.

a. Data protection and privacy

As noted in the introduction, this document does not cover an assessment of personal data protection aspects.

As general consideration, Regulation (EU) 2016/679 (the General Data Protection Regulation (GDPR))[25] applies horizontally to the processing of personal data for the purposes of preventing and fighting money laundering and terrorist financing. However, Directive 2016/680 (the Data Protection Law Enforcement Directive (LED))[26] applies to the processing of personal data by competent authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offences, and therefore applies to competent authorities investigating or prosecuting criminal offences in relation to money laundering or terrorist financing.

b. Rights of obliged entities' customers

Obliged entities are, in principle, obliged to refuse, abstain from or discontinue business relationships with specific customers when they are unable to perform appropriate customer due diligence[27]. Moreover, obliged entities, by virtue of their freedom of contract, can decide not to enter into business relationships with specific customers[28]. Therefore, when setting up a partnership, it is important that attention is paid to including provisions which would discourage obliged entities from de-risking, i.e. the suspension of a business relationship with certain clients, based on the information shared in the framework of the partnership[29].

---

[24] For further information on risks, Vogel, B., & Maillart, J.-B. (Eds.). (2020). National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection. Cambridge; Antwerp; Chicago: Intersentia.

[25] 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), OJ L 119, 4.5.2016, p. 1–88.

[26] 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, OJ L 119, 4.5.2016, p. 89–131.

[27] Article 14(4) of of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[28] Nevertheless, obliged entities are limited in their freedom of contract by the provisions of the "Payment Account Directive", i.e. Directive 2014/92/EU, which says that anyone residing legally in the European Union has the right to open a payment account with basic features in any EU country if does not have another bank account in this country, but, however, it must always comply with EU anti-money laundering rules.

[29] The European Data Protection Supervisor (EDPS) opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020: 20-07-23_edps_aml_opinion_en.pdf (europa.eu).

It is therefore essential, when designing an operational public-private partnership, that provisions on the measures to be taken by obliged entities on the basis of the information received, such as the discontinuation of the business relationship, consider the compliance of those measures with the contractual clauses and the rights and obligations of both parties.

Obliged entities are also expected to refrain from taking preventive measures that might jeopardise law enforcement authorities' activities[30], and in particular, ongoing criminal investigations. This last aspect may be considered when evaluating the interest for the obliged entity to continue the business relationship when it is in possession of information that would lead the obliged entity to take a business decision to terminate the relationship.

c. Integrity of the criminal intelligence file and protection of the staff

Public-private information sharing can potentially impact the criminal intelligence file, FIUs' analyses and compliance by obliged entities. When sharing operational data in the framework of the partnership, this is done in compliance with national rules.

Sharing of operational data often entails the disclosure of confidential information. In addition to information concerning persons and activities, the information shared may also give an insight into the investigative techniques and strategies of competent authorities. Even if confidentiality requirements are imposed on private sector staff, such as limiting the sharing of information on a need-to-know basis and only to vetted staff, or using information only for the purpose for which it has been shared, are important elements to mitigate any risks of abuse or leak.

It is also important that initiatives taken by private entities in relation to the customers about whom information has been exchanged within the partnership are agreed and authorised, in advance, with the relevant public authority to avoid jeopardising investigative actions.

Many consulted stakeholders consider appropriate safeguards on confidentiality and coordination between parties as fundamental to prevent or limit possible interferences in the criminal investigation.

The mentioned safeguards could also protect the anonymity of the staff of obliged entities involved in the sharing of information and the confidentiality of the information exchanged with public authorities. Information shared in the framework of a public-private partnership might concern, for example, organised crime groups and might be of a nature that could cause significant financial damages to the organised crime groups. This could trigger possible retaliation against the staff who participated in the public-private partnership from the side of the obliged entity.

d. The relationship between criminal investigations, FIUs and obliged entities' compliance

[30] Article 39(1) of of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

An obliged entity is already bound to provide information to a law enforcement authority when requested in the framework of a criminal proceeding and when the obliged entity suspects that a criminal offence has been/is being committed[31].

As a general rule, all investigative activities must be carried out in full respect of the rule of law, the relevant provisions of the Charter of Fundamental Rights[32], and the EU procedural rights directives[33]. Procedural rules on conducting criminal investigations are, in principle, a national prerogative.

In accordance with the national legal framework and corresponding safeguards, operational public-private partnerships may complement the collection of information within criminal proceedings by enabling the collaboration between competent authorities and obliged entities and the development of financial intelligence that can facilitate the opening of criminal investigations.

It is therefore important to ensure clarity among participants in public-private partnerships about the respective roles of investigative authorities and FIU and the difference between information gathered during a criminal investigation and the collection and dissemination of financial information produced in the context of a public-private partnership.

Insofar as the information exchanged in a public-private partnership could lead to the gathering of information for the pursuing of ongoing criminal proceedings, it is important that Member States regulate the use of such information by ensuring compliance with relevant procedural rules.

e. Competition and anti-trust

Several respondents to the Commission's open public consultation note that guidance in the area of competition law is needed in the context of AML/CFT public-private partnerships. One respondent specifies that 'competition law and anti-trust are part of the legal barriers to set up partnerships'. This could be the case where sharing of information between public authorities and certain obliged entities may provide some market participants with a competitive advantage and may lead to a distortion of competition. The contributions received in preparation of this document have not allowed to draw clear conclusions on this point.

Stakeholders can nevertheless consider whether challenges pertaining to competition law may arise in the context of exchanges of information in the framework of public-private

[31] Article 33 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[32] Charter of Fundamental Rights of the European Union (2012/C 326/02). With regard to the application of the Charter of Fundamental Rights to Member States see Article 51.1.

[33] Directive 2010/64/EU on the right to interpretation and translation, Directive 2012/13/EU on the right to information, Directive 2013/48/EU on the right of access to a lawyer, Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, Directive (EU) 2016/1919 on legal aid and Directive (EU)2016/800 on procedural safeguards for children who are suspects or accused persons in criminal proceedings.

partnerships and, if necessary, put in place safeguards to address such challenges. As a general principle, it might be appropriate to consider whether the structures put in place, and the information exchanged, do not risk facilitating anti-competitive practices on the side of the private sector, such as cartels. Similarly, consideration should be given to whether it might not strengthen the dominant position of one or other participant from the private sector in a given market (for example, by accessing privileged information that would allow the operator to act ahead of changes in the market).

7. Good practices

This document has identified a number of good practices[34] in the context of setting up public-private partnerships for the exchanges of information between law enforcement authorities, FIUs and the private sector[35]. These are covered below.

a. Putting in place a clear governance structure and objectives from the outset and involving different authorities

Establishing a clear governance structure and objectives from the outset has been noted as a good practice by stakeholders. Not all aspects and objectives can be planned from the start of the project, and a certain degree of flexibility should be envisaged to adapt to changing circumstances. Nevertheless, having a sound methodology and clear direction from the outset may enhance effectiveness and efficiency.

Moreover, as already illustrated above, public-private partnerships interact with a number of legal considerations, ranging from operational aspects to data protection to procedural safeguards. It is therefore important to ensure that certain public authorities, notably FIUs and data protection authorities, are involved in the project from the outset, including its design, to enable sharing of financial information.

b. Ensuring that there are national guidelines or regulations on the operation of the public-private partnership

Adopting guidelines or regulations setting out the terms of application of the legal framework as regards the public-private partnership would lead to greater legal certainty amongst participants as regards their respective rights and obligations and in relation to the partnership's aims and objectives.

---

[34] In addition, it is worth noting that RUSI outlines five guiding principles that may be considered when setting up a public-private partnership. These principles (leadership and trust; legislative clarity; governance; technology and analytical capability; and adaptability and evolution) are '…designed to help policymakers design, implement, evaluate and improve information-sharing partnerships in their jurisdictions.' Associated with each principle is a set of outcomes and recommendations that can be put in place to achieve such outcomes. For more information: The Role of Financial Information-Sharing Partnerships in the Disruption of Crime | Royal United Services Institute (rusi.org). Furthermore, a paper by the Wolfsberg Group on Effectiveness through Collaboration focuses on public-private partnerships and lists a number of elements to be considered for greater effectiveness. For more information: https://wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Effectiveness%20Through%20Collaboration.pdf.

[35] As indicated in the introduction, this document does not cover an assessment of personal data protection aspects.

This is the case, for example, for the Cooperation Coordination Group, led by the Latvian FIU, which has been operating since the second half of 2018[36].

c. Establishing a secure IT platform to share specific confidential documents on typologies, new threats and risks

Putting in place a channel through which confidential documents can be shared among participants is also identified as a good practice, ensuring that public authorities and private sector entities are able to collaborate and exchange confidential strategic information in a secure manner.

This is the case, for example, with the Belgian public-private partnership initiative, which has put in place such an IT tool and with the EFIPPP, where documents with typologies are shared via the Europol Platform for Experts (EPE)[37].

d. Establishing key performance indicators (KPIs) to measure the effectiveness of the respective public-private partnership

The establishment of KPIs may be a useful tool to help measure the effectiveness and outcomes of public-private partnerships. Key performance indicators may relate to:

- the number of documents with specific crime typologies, trends, patterns, or risk indicators disseminated in the context of the partnership;
- the number of STRs/SARs submitted by obliged entities (whether per sector, on a specific typology or across all obliged entities);
- improvement in the quality of STRs/SARs (more relevant and better targeted reports, greater clarity in describing suspicion, completeness of the STR/SAR and the accompanying documentation);
- the number of investigations, prosecutions and/or convictions initiated as a result of the respective public-private partnership; and
- the value of assets frozen, seized or confiscated as a result of the public-private partnership.

In the absence of KPIs, some stakeholders conduct regular reviews to assess whether the desired goals are being delivered. In many cases, it would not be possible to establish that increases in, for instance, the number of STRs/SARs or the value of assets seized are the direct result of a public-private partnership. However, such KPIs may still provide insightful information on the overall effectiveness of partnerships and outreach activities.

e. Involving non-governmental organisations, and academic and research institutions

[36] For further information on the Cooperation Coordination Group and the Regulation for its Operation, please visit Public-private partnership | Finanšu izlūkošanas dienests (fid.gov.lv).
[37] For further information on the EPE, please visit Europol Platform for Experts (EPE) | Europol (europa.eu).

Non-governmental organisations and academic and research institutions, including think-tanks, may contribute to some aspects of public-private partnerships, depending on their area of work and the subject-matter of the partnership. Certain organisations may have insight on specific risks and activities (e.g. trafficking in human beings, wildlife trafficking, corruption) that may supplement the knowledge of FIUs and law enforcement authorities on a given criminal behaviour, particularly in relation to work on the development of red flags and typologies.

8. Conclusions and next steps

Public-private partnerships have become increasingly important fora for cooperation and information exchange between FIUs, various national supervisory and law enforcement authorities and obliged entities. As shown in this document, public-private partnerships can complement the existing anti-money laundering and countering the financing of terrorism framework and improve obliged entities' understanding of the risks in this regard and strengthen their detection systems. This can ultimately lead to swiftly detected and identified illicit financial flows and better quality STRs/SARs submitted to FIUs, which can then disseminate their analysis to national law enforcement authorities. This will ensure that illicit financial flows are swiftly detected and identified, and ultimately that assets are frozen, seized and confiscated so that crime does not pay.

At the same time, as detailed in section 6 of this document, there are a number of considerations to be taken into account in the setting-up and operation of public-private partnerships.

The scale of the money laundering phenomenon and the threat it poses to our society and economy remain significant and require common efforts by obliged entities, FIUs and law enforcement authorities. The challenge is also significant in relation to terrorism financing, where obliged entities struggle to detect financial movements that are often of low value and of a seemingly legitimate nature. Public-private partnerships have the potential to provide obliged entities with guidance that allows them to refine their detection systems or with targeted information that enables them to find 'the needle in the haystack'. When setting up public-private partnerships as a complementary tool in the fight against money laundering and terrorist financing, it is important that Member States take into account the best practices collected in this staff working document and the legal considerations that are necessary ensure the respect of fundamental rights.

The Commission will continue to closely monitor relevant developments in the area of public-private partnerships for the prevention and fighting of money laundering and terrorist financing and continue the engagement with public and private stakeholders in relevant

expert groups, networks and other meetings[38], in order to encourage where appropriate the role of public-private partnerships in facilitating better use of information.

ANNEX

STAKEHOLDER CONSULTATION - SYNOPSIS REPORT
of the consultation activities with regard to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing

1. INTRODUCTION

The effective exchange of information is crucial in the fight against money laundering and terrorist financing (ML/TF). Public-private partnerships (PPPs), established to exchange information between competent authorities (e.g., Financial Intelligence Units (FIUs), law enforcement authorities, and even supervisors) and the private sector (obliged entities) can take various forms. Some partnerships are established to exchange strategic information on typologies, trends and patterns between FIUs and obliged entities; others involve the sharing between law enforcement authorities and obliged entities of operational information on persons of interest, for the purposes of monitoring transactional activities.

The Commission's action plan for a comprehensive Union policy on preventing ML/TF[39] notes that in the context of making better use of financial intelligence, the role of public-private partnerships should be encouraged to the extent possible.

To gather perspectives and evidence, a consultation exercise was undertaken among various stakeholders between June and November 2021. This synopsis report presents an overview of the consultation process and the feedback received.

[38] Including the EU FIUs' Platform, the Network of Counter-Terrorism financial investigators, the Anti-Money Laundering Operational Network (AMON), the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and international conferences.

[39] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (2020/C 164/06)

2. THE CONSULTATION PROCESS

As outlined in the consultation strategy[40], the objective of the consultation was to collect views and opinions about:

- the types of public-private partnerships currently operating in EU Member States in the area of ML/TF prevention;
- the types of authorities and entities that participate;
- the types of information exchanged and the measures to safeguard fundamental rights;
- the mechanisms in place to measure the effectiveness;
- the impact and added value of such partnerships;
- good practices in the development and operation of public-private partnerships; and
- challenges faced by the authorities and entities participating in such partnerships.

This was done through an open public questionnaire on the European Commission's 'Have Your Say' portal, and a closed consultation of the EU FIUs Platform, an expert group of the European Commission.

Contributions received through consultations cannot be regarded as the official position of the Commission and its services. They do not, therefore, bind the Commission. Additionally, the contributions cannot be considered as a representative sample of the EU population.

Throughout this report, responses to multiple-choice questions are presented statistically, while responses to open questions are summarized and explained verbally.

3. RESPONSE TO THE CONSULTATION

a. Open public consultation through the Have Your Say portal

Overview

The consultation targeted all interested stakeholders from both the public and private sector. In addition to responses from the general public, and associations representing a broad range of citizens (e.g.: consumer associations, trade unions), the consultation sought to receive responses from:

- public authorities in Member States (e.g.: FIUs, law enforcement authorities, supervisory authorities, data protection authorities, ministries dealing with criminal proceedings);
- private sector entities (e.g.: entities required to apply rules on anti-money laundering and countering the financing of terrorism (AML/CFT) under the Anti-money Laundering Directive, and their representative organisations);

[40] Consultation strategy: Commission guidance on the rules applicable to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing | European Commission (europa.eu)

- EU bodies and agencies (e.g.: the EU Agency for Law Enforcement Cooperation (Europol) the European Banking Authority (EBA), the EU Agency for Fundamental Rights (FRA), Eurojust);
- academic organisations, research institutions and think-tanks;
- non-governmental organisations (NGOs); and
- international organisations

The questionnaire was available in 23 EU languages. Respondents could contribute to all or some of the questions, and could submit additional documentation.

Profile of respondents
Responses came from individuals (13% of responses), business associations (24%), companies or business organisations (21%), public authorities (13%), NGOs (8%), academic/research institutions (5%), trade unions (3%), while 13% were uncategorised.

Out of the 38 contributions received, 13% were from people identifying as EU citizens. The remaining respondents were distributed across different sized organisations; 29% from small organisations (between 10-49 employees), 26% from large organisations (250 or more employees), 21% from medium organisations (50-249 employees), and 11% were from micro organisations (1-9 employees).

Contributions were received from 20 different countries. These included 16 EU Member States and 4 non-EU countries.

The banking sector accounted for 21% with the remaining responses distributed across sectors such as accounting, auditing, consulting, legal services, tax advice, notarial services, insurance and other financial services, think tanks and consulting bodies, and from the gambling industry. Some respondents (34%) did not indicate their field.

Twelve additional papers were submitted together with responses.

Contribution of EU agencies
One contribution to the open public consultation was received on behalf of Europol.

Contributions of national bodies
Four contributions were from Member State Financial Intelligence Units. Another contribution was received on behalf of a number of bodies involved in the AML/CFT framework of another Member State.

Summary of responses
The open public consultation questionnaire consisted of 23 sets of questions, comprising multiple choice questions, selection lists, and open questions. In summary, respondents were asked about their perspectives on various aspects of public-private partnership (PPPs), their experiences with PPPs set up in their country, and the legal barriers and potential risks of such partnerships.

The following sections provide a high-level summary of the various responses received.

The exchange of information in the fight against ML/TF

Some 83% of respondents support the view that partnerships between public authorities and private sector entities are needed in order to prevent and fight ML/TF effectively. Respondents indicated that PPPs increase capabilities to prioritize threats and pool resources, improve awareness of criminal trends and behaviour, and enable more effective, targeted and efficient action to prevent, detect and combat threats. These benefits were considered to apply to both competent authorities and private sector operators. Many respondents consider that such exchanges promote an improvement in suspicious transaction reporting by obliged entities, in terms of:

- an increase in the number of suspicious transaction reports (STRs) on specific, current threats;
- an increase in the quality and utility of STRs; and
- more timely and relevant reporting.

Respondents mentioned the need for guidance on the exchange of operational information in conformity with privacy and data protection rules, and on the measurable actions and goals that PPPs ought to pursue. One respondent suggested using PPPs as fora to test technological solutions. Some respondents (5%) were less keen on having PPPs for the exchange of information between competent authorities and the private sector.

Partners in public-private partnerships

Respondents were asked to select from a list those public authorities that should participate in PPPs. The most selected response (16 respondents) was the one that included the widest range of authorities, namely FIUs, law enforcement authorities, AML/CFT supervisors, customs and tax authorities, and asset recovery offices. Respondents suggested the inclusion of other bodies, such as prudential supervisors, secret services, and company registries, depending on the type of information being exchanged.

With respect to private sector bodies, just under half of respondents (49%) selected all the listed categories of obliged entities as ideal participants, which suggests that PPPs ought to cover a wide range of sectors. Following that, 8% of respondents consider that only financial institutions, credit institutions, and virtual asset service providers should participate. While all other responses varied from each other, every respondent selected financial institutions. Some respondents suggested criteria to define membership eligibility in PPPs, such as the objectives of the partnership itself, and the sensitivity of the case within operational partnerships.

Some 86% of respondents believe that NGOs, academic organisations and research institutions should be involved in discussions on the design of PPPs, although to a limited extent. Elaborating on their choice, some respondents consider NGOs to possess useful knowledge on criminal activities and may aid in the creation of sector-specific typologies.

Public-private partnerships in the EU

Some 57% of respondents stated that there is a PPP established in their country. Many of these share the primary objective of enhancing the ability of both the private and public sector to combat ML/TF more effectively, through dialogue, sharing information, and by working together to develop typologies. The type of information exchanged is mainly strategic; however, some of the respondents also indicated that partnerships share case-specific information.

Security measures and vetting procedures implemented by such PPPs include screening of members, the implementation of processes for new membership, data retention periods, and the involvement of privacy experts to ensure that information is exchanged in full respect of existing legal frameworks.

Respondents noted the positive impact of PPPs, including better trust and cooperation among the private sector and competent authorities, better understanding of FIU needs and expectations, and swifter responses and better-quality reports from obliged entities.

Respondents shared good practices that may be implemented, notably building trust with partners, and ensuring that all members cooperate equally. Other suggestions include prioritizing projects in advance to ensure focus and efficiency, assessing capacity and planning work in line with available resources, and following a transparent and agreed-upon methodology. One respondent recommended the establishment of key performance indicators to measure the results of the PPP. Another advised that PPPs should initially be small in size and then develop over time.

Legal barriers, risks and consequences

Asked if they are aware of legal barriers that may hinder the setting up of PPPs, some respondents explained that legislation does not always enable information to be shared multilaterally or in a private-to-private sector framework. Additionally, stakeholders may not be willing to share information in view of perceived risks of breaching AML/CFT and privacy rules. Banking and insurance secrecy laws, competition law, privacy and data protection rules, and non-disclosure laws within the AML/CFT context, were those most mentioned as posing a barrier.

The consultation sought to assess whether respondents have experienced negative consequences resulting from PPPs. While some respondents did not notice any negative consequences, others mentioned de-risking, although it was clarified that PPPs provide an opportunity to develop clearer, more concrete indicators that allow obliged entities to adopt a more nuanced understanding of risk.

PPPs for the exchange of strategic information

Information was specifically sought on PPPs that share strategic information, i.e. sanitised information on trends and typologies.

Respondents were asked to select the objectives that such PPPs ought to pursue and 60% of respondents selected all the suggested objectives, listed below:

- sharing of strategic information to enhance the understanding of ML/TF risks;
- improving the quality of suspicious transaction reporting by obliged entities;
- preparation of risk indicators and red flags to improve detection by the private sector;
- work on risk mitigation measures related to specific ML/TF risks; and
- joint capacity building/training activities and provision of technical assistance

Respondents proposed other objectives, including rapid identification of new modi operandi, strengthening networks between participants, improving the AML/CFT legislative framework, and discussing developments in technology.

Based on their experience, 71% of respondents believe that such partnerships have a positive or very positive impact on fighting ML/TF, 8% believe they have a negative or very negative impact, while the remaining respondents were neutral. Risks concern profiling of specific individuals or groups of people, breaches of official secrecy and disclosure of sensitive information. Bank secrecy, social and economic exclusion and legal privilege were also a concern. Some respondents indicated that risks are more limited for strategic exchanges than for operational ones, while guidance and proper legal frameworks may mitigate such risks.

Respondents believe that guidance is needed on rules regarding the protection of fundamental rights (e.g. data protection and privacy) (68% of respondents), the provision of feedback on STRs (63%), and antitrust rules (40%). Other areas mentioned include guidance on key performance indicators, governance and the use of technology.

PPPs for the exchange of operational information

Part of the questionnaire sought to obtain insights on PPPs set up for the exchange of operational information. Asked to select the objectives that such partnerships should pursue, respondents selected as follows: mapping of criminal networks, based on the sharing of operational information by competent authorities (74% of respondents), obtaining leads in the context of criminal investigations (68%), and monitoring transactions of persons of interest prior to the initiation of a formal criminal investigation (68%). Respondents also selected the following objectives: identifying persons of interest prior to the initiation of a formal criminal investigation (60%); and obtaining evidence on suspects in criminal investigations as a main objective (45%).

Based on their experience, 51% of respondents believe that such partnerships have a positive or very positive impact on fighting ML/TF, 9% believe they have a negative or very negative impact, while remaining respondents were neutral or did not provide their view.

Operational partnerships envisage the exchange of sensitive information including names and transactional data of people suspected to be involved in ML/TF. Asked where they would see risks, respondents pointed to risks to fundamental rights (the rights to the protection of personal data and privacy and the presumption of innocence being those most relevant in this context) (selected by 80% of respondents). Other risks were selected as follows: official secrecy and the disclosure of sensitive information on ongoing criminal proceedings (54% of

respondents), bank secrecy (37%), social and economic inclusion (37%), legal privilege (31%), and the integrity of ongoing proceedings (31%).

These views are reflected in the replies to questions on which rules require the most guidance: rules on fundamental rights (74% of respondents), applicable criminal procedural rules (51%), and antitrust rules (26%).

Transnational partnerships

Transnational public-private partnerships bring together stakeholders from multiple countries. Some 63% of respondents believe that both operational and strategic information may be exchanged within such partnerships.

Some 20% of respondents believe that transnational partnerships should only be used to exchange strategic information, with concerns raised on the legality of sharing operational information transnationally. Finally, 8% of respondents believe that transnational partnerships should be set up to exchange only operational information.

Some do not see major differences between national and transnational partnerships, although emphasis was made on ensuring that the legal frameworks of all participating countries are respected.

Respondents broadly consider transnational PPPs to be a useful tool in the fight against ML/TF. Asked to select the main benefits from a list, 86% of respondents believe that transnational PPPs would lead to a better understanding of the cross-border risks associated with ML/TF. Similarly, 83% of respondents consider that such PPPs can lead, on the one hand to an improvement in the private sector's ability to detect cross-border suspicious financial flows, and, on the other, to more effective cross-border financial investigations into ML/TF.

Regarding the risks of such partnerships, the most selected one relates to the protection of personal data and privacy, selected by 74% of respondents, followed by fundamental rights including the presumption of innocence (54%) and official secrecy and the disclosure of sensitive information related to ongoing criminal proceedings (51%). Other risks were of a somewhat lesser concern, namely bank secrecy (40%), social and economic inclusion (31%), the integrity of ongoing criminal proceedings (28%) and legal privilege (27%).

b. Position papers

Twelve respondents submitted additional documentation with their responses. The following section summarises key points and recommendations emerging from these documents.

Responses indicate that PPPs encourage a common purpose based on shared interests, and help to develop a collaborative relationship. One paper, based on a study of 20 existing information sharing partnerships across the world, explains that PPPs enable private sectors entities to provide more targeted and timely reports, while the public sector broadens its

understanding of complex financial issues. PPPs may also improve risk understanding in situations where national risk assessments are not up to date.

One paper sets out how PPPs tend to have one of two objectives: to serve ongoing investigations or to support compliance and reporting efforts of obliged entities. The set-up and the information exchanged will vary depending on the objective.

Further aspects affecting PPPs

Responses indicate that there are additional aspects that need to be addressed to enable effective and sustainable partnerships for exchange of information, notably concerning data protection, procedural safeguards and de-risking. The majority of views set out in this section were provided in response to open, free-text questions, and are therefore provided as qualitative reflections without statistical figures.

With respect to data protection, a primary concern is the potential for incoherence of legislative priorities between financial crime and data protection. Some responses call for policy makers to consider the sharing of operational information in the context of PPPs as fulfilling a 'legitimate interest' in the context of Regulation 2016/679 (General Data Protection Regulation). On the other hand, it was highlighted that the non-disclosure obligations surrounding STR information affects the ability of data subjects to exercise their rights of access. A recommendation was made to mandate formal cooperation between AML/CFT and data protection authorities.

De-risking remains a cause for concern; information shared with the private sector may potentially lead to de-risking of broad categories of clients if it does not contain sufficiently detailed indicators. On the other hand, PPPs are themselves a mechanism for providing better risk indicators, in turn lessening the de-risking phenomena.

The use of FIUs as a de facto investigative tool is also seen as an obstacle to safeguards under judicial processes, such as judicial authorization or oversight of the requisition of documents used as evidence.

Some respondents consider that risks may be mitigated through the implementation of safeguards, including vetting participants, clear guidance on the use of data, the use of secure channels, and formal governance structures.

Some respondents consider the above risks to be unlikely to materialize within PPPs set up for the exchange of strategic information. In view of this low risk, some respondents call upon the Commission to encourage all Member States to establish a PPP for the exchange of strategic information. Similarly, it was suggested that the exchange of information ought to be made a policy priority and an essential part of the AML/CFT framework, providing a basis for better allocation of resources to participate in the work of PPPs.

Feedback on suspicious transaction reports

Providing feedback on the quality and use of STRs was seen as an important element in the exchange of information framework. A lack of feedback from FIUs is seen as preventing a

focus on transactional activity that is relevant to FIUs. An enhanced feedback regime may reduce the number of false positives. It is suggested that the scope and depth of the feedback obligation be made clearer.

Measuring impact
Respondents suggested criteria that PPPs may adopt to measure the impact of their work. Such criteria can include:

- value of assets seized;
- number of arrests;
- number of suspect accounts identified;
- number of investigations initiated;
- number of victims identified; and
- value of fraud loss prevented.

Transnational PPPs
Members of a transnational PPP submitted feedback on cross-border and domestic anti-financial crime PPPs. They highlighted their objectives and value, challenges to cooperation, and provided recommendations on improving PPPs. The feedback explains how the typologies produced within the transnational PPP are being used by both the private and public sector to improve transaction monitoring and the identification of cases respectively. Respondents consider that the inconsistent interpretation of legal frameworks for data protection, use of STR information, and bank secrecy may be preventing the sharing of information, both domestically and across borders. Recommendations are made with respect to improving feedback from FIUs, and encouraging the establishment of PPPs in all Member States.

c. Closed consultation of the EU FIUs Platform

Recognising EU FIUs as important stakeholders in the AML/CFT framework, the Commission distributed a questionnaire among members of the EU FIUs Platform – the expert working group of the European Commission composed of EU and EEA FIUs and a number of observers. Fourteen FIUs submitted responses and Europol submitted a position paper based on its experiences with the Europol Financial Intelligence Public Private Partnership (EFIPPP).

The responses reflected that established PPPs have resulted in better cooperation between the private sector and competent authorities, a better understanding of FIU needs and expectations by obliged entities, and in turn, higher quality reports from obliged entities.

Respondents described the nature of the information exchanged within the partnership, listed some of the challenges faced, and provided best practices. Planned developments include broadening partnerships to involve new sectors, establishing additional smaller partnerships, involving supervisory bodies, and disseminating more information reports.

4. CONCLUSIONS AND NEXT STEPS

The consultation process represents an important step for the Commission with a view to obtaining perspectives and experiences of the various stakeholders involved in the AML/CFT framework. The outcomes of the consultation will support the drafting of a commission staff working document on the rules applicable to the use of public-private partnerships for the exchange of information. While the synopsis report provides a broad summary of the responses received, the individual responses and position papers submitted provide valuable insight.

The next steps will see the Commission adopting a document to assist Member States in setting up public-private partnerships that facilitate the exchange of information within the applicable legal frameworks, enhancing the effective prevention of and fight against ML/TF, while protecting fundamental rights at all times.