

# Public consultation on guidance on the rules applicable to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing

Fields marked with \* are mandatory.

## Introduction

---

This consultation is now available in 23 European Union official languages.

Please use the language selector at the top of this page to choose your language for this consultation.

The effective exchange of information is crucial in the [fight against money laundering and the financing of terrorism \(AML/CFT\)](#). This includes not only the exchange of information between public authorities (e.g. financial intelligence units (FIUs), law enforcement authorities and supervisory authorities), but also the exchange of information between authorities from the public sector and private sector entities.

The [Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorist financing](#) 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 as in some cases the nature of the information might limit its sharing and such sharing must comply with the data protection legal framework and with other rules. Public-private partnerships entail the sharing of information between competent authorities and the private sector and can take various forms. Some are limited to the exchange of information on, for example, typologies, trends and patterns by FIUs to obliged entities, whilst others pertain to the sharing of operational information and intelligence on suspects by law enforcement authorities to obliged entities for the purposes of monitoring the transactions of these suspects. The current EU AML/CFT framework (the [4<sup>th</sup> Anti-Money Laundering Directive](#)) already requires FIUs to provide feedback, where practicable, to obliged entities on the usefulness and follow-up of the suspicious transaction reports.

Due to differences in the legal frameworks and practical arrangements across the EU Member States, the Commission considers it essential to provide guidance and share good practices for public-private partnerships in relation, in particular, to antitrust rules, safeguards and limitations in relation to data protection and guarantees on fundamental rights. In the May 2020 action plan, the Commission also announced that it will consider the possibility of requesting the [European Data Protection Board \(EDPB\)](#) to issue an opinion as regards the data protection aspects of public-private partnerships.

In this context, and in line with the [better regulation principles](#), the Commission is herewith inviting stakeholders to express their views. The consultation aims to obtain information with regard to, for example

- the types of public-private partnerships currently operating in the EU Member States in the area of preventing and fighting money laundering and terrorist financing
- the public authorities (e.g. FIUs, law enforcement, supervisory authorities) and private sector entities which participate
- the types of information exchanged within those partnerships and the measures put in place to guarantee the preservation of fundamental rights
- the mechanisms put in place to measure the effectiveness and success of those partnerships (e.g. key performance indicators (KPIs) or any other performance metrics)
- the impacts and added value of the various public-private partnerships in the fight against money laundering and the financing of terrorism
- the impacts on fundamental rights, including the presumption of innocence, as well as on the due process of criminal proceedings
- good practices in the development and operation of public-private partnerships
- potential obstacles to the exchange of information and challenges faced by the authorities and entities participating in public-private partnerships in the area of preventing and fighting money laundering and terrorist financing and what do they pertain to

The outcome of this public consultation will provide the Commission with sufficient information and evidence for the purposes of preparing the guidance on the rules applicable to the use of public private partnerships in the framework of preventing and fighting money laundering and terrorist financing and issue best practices in Q4 2021.

---

**Please note:** In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact [fisma-financial-crime@ec.europa.eu](mailto:fisma-financial-crime@ec.europa.eu).

More information on

- [this consultation](#)
- [the consultation document](#)
- [the consultation strategy](#)
- [anti-money laundering and countering the financing of terrorism](#)
- [on the protection of personal data regime for this consultation](#)

## About you

---

\* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Irish
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

\* I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)

- Public authority
- Trade union
- Other

\* First name

Iryna

\* Surname

de Smedt

\* Email (this won't be published)

iryna@accountancyeurope.eu

\* Organisation name

*255 character(s) maximum*

Accountancy Europe unites 51 professional organisations from 35 countries that represent 1 million qualified accountants, auditors and advisors

\* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

*255 character(s) maximum*

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

4713568401-18

\* Country of origin

Please add your country of origin, or that of your organisation.

- Afghanistan
- Åland Islands
- Djibouti
- Dominica
- Libya
- Liechtenstein
- Saint Martin
- Saint Pierre and Miquelon

- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden

- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States

- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena
- Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

\* Field of activity or sector (if applicable)

- Accounting
- Art dealing
- Auditing
- Banking
- Company and trust creation and management
- Consulting
- Gambling
- Insurance
- Investment management (e.g. assets, securities)
- Other company and trust services
- Other financial services
- Notary services

- Legal services
- Pension provision
- Real estate
- Tax advice
- Think tank
- Trading in goods
- Virtual assets
- Other
- Not applicable

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association', 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

#### \* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

##### Anonymous

Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

##### Public

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

I agree with the [personal data protection provisions](#)

## I. Context

---

**Question 1. In which ways do you consider that the exchange of information between competent authorities and private sector entities can contribute to the prevention of and fight against money laundering and the financing of terrorism?**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Analysis of typologies and the feedback on Suspicious Activity Reports (SARs) are essential to prevent money laundering/terrorist financing (ML/TF) proliferation. Exchange of information about trends, patterns and typologies will identify red flags on matters that otherwise may have not appeared concerning.

Working together to understand better how criminals use the financial and non-financial sector will result in better Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) risk management. The exchange of information between competent authorities and private sector entities is key to prevent or assist in detecting crime. For example, some of the operational Joint Money Laundering Intelligence Taskforce (JMLIT) work around the pandemic relief schemes, known as a 'fusion cell', highlighted Organised Crime Group's involvement in exploiting these relief schemes.

Financial Intelligence Units (FIUs) have a crucial role in assessing trends in ML and TF across the EU to identify common elements and typologies. Information and intelligence sharing by FIUs can also significantly contribute to the EU AML supervisor's work. Cooperation with the obliged entities (OEs) and real-time information exchange would help spot trends and identify typologies. To this end, there needs to be further collaboration and exchange of information between the FIUs and OEs in the financial and non-financial sector.

Information needs to be shared in a timely manner and on a two-way basis (from the private sector to the law enforcement and the other way around). This will help to ensure that knowledge on trends and typologies is up to date considering that money laundering landscape changes very quickly and criminal activity also evolves very quickly.

**Question 2. Have any formal and/or informal mechanisms been put in place in your country (in the case of private sector entities, 'country' is to be understood as place of operation) in order to increase cooperation and exchange of information between competent authorities and private sector entities to prevent and fight money laundering and the financing of terrorism?**

- Yes
- No
- Don't know / no opinion / not applicable

**Please explain your answer to question 2:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The accountancy profession generally is not included to any great extent in this type of partnerships. Consequently, in many jurisdictions the profession's PPPs experience is limited. Nonetheless, the profession would welcome being part of the PPPs.

Accountancy Europe is an EU based association, and its input reflects our members' joint positions. Nevertheless, for this specific question we believe national input will be of use for the EC. We also included feedback based on the UK PPPs experience as the UK has been engaged in PPPs the longest and is one of the only/few countries where accountants are involved in intelligence sharing. Relevant examples stemming from this experience are also included under several other consultation questions.

We include several national examples in an Annex attached to this survey.

**Question 3. In your view, what does a 'public-private partnership' mean in the context of preventing and fighting against money laundering and the financing of terrorism?**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

PPPs play a vital role in strengthening the overall AML ecosystem. For the accountancy profession, being part of a PPP helps to better understand the emerging threats that could impact their sector. This collaboration allows accountants to factor these insights into their risk assessment of prospective clients and engagements. Namely, risk indicators and red flags can be built into firms' systems and controls to adopt appropriate risk mitigation measures.

PPPs should be tailored to consider sector specific specificities

We welcome PPP collaboration and would like to assist in creating a form of partnership which will work for non-banks. The EC should ensure that its guidance on the rules applicable to PPPs is tailored to accommodate different actors in the AML ecosystem and in particular the accountancy profession.

Otherwise, there is a great risk the rules on PPPs would be designed mainly for financial entities and unsuited for other sectors and professions. We have seen examples of that with the AML directives which were primarily written for banks and contain requirements which are not adapted to the nature of the auditor's engagement.

The rules should acknowledge that there are different types of OEs and consider how PPPs should allow for their respective participation. A concrete example how the EC guidance should consider the specificities of the non-financial sector relates to strategic information sharing. If the purpose is sharing information based on the analysis of large sets of transactional data, this objective would not be applicable in the context of the accountancy profession.

The profession does not hold vast transactional data pools as is the case for banks. In this respect, large financial institutions with access to data analytics may have capacity for more advanced information sharing.

The accountancy profession due to the nature of their services can contribute with typologies and red flags. Their work on audits, tax work and other services may result in valuable insights and assist in building a richer picture of how bad actors move through the regulated sector. However, compared to financial institutions they often do not have an ability to see the immediate money laundering asset flows in action, but rather pick it up at a later stage.

Consequently, the EC guidance should provide clarity what type of data the strategic information should encompass. We further elaborate on this point in our reply to Question 11.

PPPs should promote collaboration and information exchange

The concept of collaboration extends beyond cooperation. For example, collaboration involves accountants, national competent authorities and other relevant parties in an active role, working together with the authorities, inputting examples to develop typologies. Cooperation implies a less active role such as sharing data e.g. responding to enquiries, filing STRs/SARs.

We see two essential levels of information exchange in the PPP context (1) vertical level - between private sector and governmental institutions and (2) horizontal level among the private sector players. They both are critical to ensure the AML/CFT efficiency.

**Question 4. Are you of the opinion that partnerships between public authorities and private sector entities are needed in order to prevent and**

## fight money laundering and the financing of terrorism efficiently and effectively?

- Yes
- No
- Don't know / no opinion / not applicable

### Question 4.1 If you answered 'yes' to question 4, please explain why and provide examples:

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Public authorities should overcome the 'taboo' of cooperating with the private sector to combat financial crime. Although this practice seems to be more established in the financial sector, this is not the case for OEs in other sectors and especially the non-financial sector. PPPs with other regulated sectors need to be established i.e. accountants, auditors, lawyers, real estate, gaming sector. Flexibility and adaptability should be the key features of such cross sectoral collaboration.

These PPPs may differ from those established with financial institutions; however, they are equally valuable in understanding how criminals abuse the financial system. Getting insight into how criminals use the regulated sector can be very informative and help firms devise better procedures and controls supporting their "gatekeeping" role.

Experience in various jurisdictions has shown that one of the PPPs' practical benefits is a greater mutual understanding of the threats. Such partnerships also allow to build a clearer picture of how bad actors move across the system. A practical example relates to one of the laundromats where the corrupt PEPs used third parties to 'front' investments. In this case, the Designated Non-Financial Businesses and Professions (DNFBPs) were able to evidence this through information they saw and thus give meaning to the transactional data and develop a series of red flags to disseminate to others in the sector.

All stakeholders in the AML/CFT ecosystem need to collaborate. Cross-sectoral collaboration will help to collectively tackle and reduce ML and TF related activities. It will facilitate asset freezes' procedures, prevent the use of the gatekeepers' services and encourage sharing best practices and typologies.

The UK's Economic Crime Plan Statement of Progress includes some useful examples of benefits from information sharing across the public and private sectors (see Strategic Priority 2: Better information sharing on p. 15):

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/983251/Economic\\_Crime\\_Plan\\_Statement\\_of\\_Progress\\_May\\_2021.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf)

The EU should further reflect on how to formalise PPPs by setting up covenants on how to share cases in a more structured way as well as root causes and learning points. In addition, a legal evaluation should be carried out on how to safely share entity information on a non-anonymous basis. The Egmont Group has set out the challenges that need to be addressed in setting up PPPs, see <https://egmontgroup.org/en>.

### Question 5. In your view, in case a public-private partnership is set up to prevent and fight money laundering and terrorist financing, which of the following public authorities should take part?

Please select as many answers as you like

- Financial intelligence units (FIUs)
- Law enforcement authorities
- Prosecution authorities
- Anti-money laundering and countering terrorist financing supervisory authorities
- Customs authorities
- Tax and recovery administration authorities
- Asset recovery offices (AROs)
- Other

**Please specify to what other authority/ies you refer in your answer to question 5:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Among the other bodies who can contribute usefully to PPPs but are not mentioned in the above list are the public registries, the social security departments, State Revenue Service, Supervisory Bodies such as the European Central Bank, European Banking Authority, National Competent Authorities, AML expert groups from the secretary of internal affairs.

**Question 5.1 Please explain why you provided that/these answer(s) to question 5 and further elaborate:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

PPPs should be cross-sector, involving all public authorities who have a role in the fight against ML such as law enforcement agencies, FIUs and other relevant public authorities, financial institutions and other private-sector organisations. Please see also our reply to Q 4.1 about the benefits of collective and cross-sectoral approach. For example, in Latvia there is a good co-operation with FIU, but there is no exchange of information with law enforcement agencies and the State Revenue Service.

In setting up a PPP, the key question should be whether all public authorities need to be represented in every aspect of public private sector collaboration. Experience in different jurisdictions indicates that a single model of PPP will not work across all sectors, even though the engagement of all sectors will significantly strengthen the intelligence landscape. We believe that the PPPs can work under various compositions depending on the objective and the task at hand.

It is important to recognise that the role each actor plays in the AML ecosystem differs as well as the resources available to them. The PPP mechanisms should be accountable and transparent while governance should be reviewed by authorities at recurring stages. When these partnerships are set up, it will be essential to ensure that their meetings remain effective, and their objectives are delivered on.

The UK's Economic Crime Strategic Board is an example how the PPP governance can be arranged. According to the Economic Crime Plan, the Economic Crime Strategic Board sits at the top of the economic crime governance. The Board includes cross-sectoral government and private sector representation at senior cabinet minister and chief executive level. The Board drives the public and private sector response to economic crime by setting shared strategic priorities for tackling economic crime and ensuring resources are aligned to deliver on these priorities. The Board also holds the economic crime system to account for performance against the strategic priorities (see the Economic Crime Plan, section 9.1.): <https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version>).

The Public Private Steering Group assists the Economic Crime Strategic Board. This Steering Group is jointly chaired by the Home Office, HM Treasury and UK Finance and has also the DNFBPs representatives. The Economic Crime Strategic Board considers the strategic priorities, develops and oversees the related strategies in the context of the economic crime plan. The day-to-day operation of intelligence sharing is carried out through a part of the National Crime Agency, known as the National Economic Crime Centre. "Cells" or working groups are agreed (and therefore given resources) by agreement of the Public Private Oversight Board and the accountancy sector has a place on that Board.

## **Question 6. In your view, in case a public-private partnerships is set up to prevent and fight money laundering and the financing of terrorism, which of the following private sector operators should participate?**

Please select as many answers as you like

- Financial institutions
- Credit institutions
- Auditors, external accountants and tax advisors
- Notaries and other independent legal professionals
- Trust or company service providers

- Virtual asset service providers (VASPs)
- Estate agents
- Traders in goods
- Providers of gambling services
- Other, e.g. telecom operators

**Question 6.1 Please explain why you provided that/these answer(s) to question 6 and further elaborate:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As for public authorities, similarly for the private sector stakeholders all the above categories should be able to participate separately in PPPs depending on the PPP's needs and the objectives.

OEs can improve their risk awareness through discussion with other private sector actors of the AML ecosystem. This collaboration is key to increase awareness of trends, indicators and recent AML developments. A representative example is the Flag It Up campaign in the UK where the accountancy, legal and real estate profession partnered with the government to exchange best practice on due diligence and SARs.

We welcome collaboration with other private sector operators and would like to assist in creating a form of partnership which will work for non-banks. The accountancy profession does not hold vast transactional data pools as is the case for banks. However, their work on audits, tax work and other services may result in valuable insight into typologies and assist in building a richer picture of how bad actors move through the regulated sector.

The non-financial sector due to the nature of their services can offer a different type of intelligence that can recognise criminal activity from different angle than the financial sector. This includes analysis of how particular crime types may seek to use the DNFBPs' services and which services are most attractive. Consequently, this analysis can improve the development of sector specific typologies and red flags, which can be used to improve the DNFBPs' gatekeeper activities and increase the reports.

Collaboration with other private sector operators can help improve the understanding of the sector specific risks. Each sector may pose different risks and red flags may vary when dealing with customers and clients.

**Question 7. In your opinion, how do public-private partnerships interact with private-to-private information sharing within a group or between private sector entities in general?**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Private to private information sharing is very useful but challenging due to client and professional confidentiality requirements and data protection issues. Sharing of information between private sector actors is usually run through the FIU which is entitled to decide on lifting potential protections.

Exchange of information on common clients within the private sector is one example of such interaction - subject to respective privacy protections. Currently very few accountancy firms would be part of such group mainly due to professional confidentiality obligations and the GDPR, which prohibits sharing information (unless crime exemption applies).

With due consideration of data protection issues, the EC should further encourage the exchange of information between obliged entities. There should be no restrictions to share information at a group level as already highlighted in the new AML regulation and FATF papers.

**Question 8. In your view, to what extent should non-governmental organisations (NGOs), research and academic institutions be involved in discussions about setting up and design of public-private partnerships to prevent and fight money laundering and the financing of terrorism?**

- They should be extensively involved
- They should be involved to a limited extent
- They should not be involved at all
- Don't know / no opinion / not applicable

**Please explain your answer to question 8:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe the entities that have first-hand and direct experience with PPPs such as FIUs, law enforcement authorities, tax authorities and OEs should be prioritised in discussions on the PPPs set-up and design. Having a direct and first-hand experience, these actors will be able to contribute insights and suggestions rooted in practice on what works and what does not work.

Contributions by NGOs, research and academic institutions is highly welcome as well in cases of collecting and analysing data e.g. European, national and sectoral risk assessments. Being objective observers, they can share the collected data that can be used as international benchmarks and exchange of best practice.

## II. Existing national experience and practices

---

**Question 9. Has a public-private partnership been established in your country in order to fight and prevent money laundering and/or the financing of terrorism?**

- Yes
- No

- Don't know / no opinion / not applicable

**Question 10. Are you aware of any legal barriers that exist in your country when it comes to setting up a public-private partnership in the framework of preventing and fighting money laundering and the financing of terrorism?**

- Yes
- No
- Don't know / no opinion / not applicable

**Please explain your answer to question 10:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In our experience, professional obligations of client confidentiality, legal privilege, the GDPR, competition law and anti-trust are part of the legal barriers to set up a PPP.

The EC will need to ensure the PPPs' legal framework allows for information and data exchange without breaching law or compromising competition related issues. Especially in cases of cross-border cooperation, the legal framework needs to provide clarity on issues such as data sharing, processing, disclosure, storage, usage etc.

In addition, lack of resources may also act as a barrier to set up a PPP. Many DNFBPs are small entities with limited data or experience which may contribute to a reluctance to get involved.

### **III. Public-private partnerships for the exchange of strategic information (e.g. typologies, trends, patterns, risk indicators, feedback to suspicious transaction reports)**

---

**Question 11. In your opinion, what should be the main objectives of a public private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Sharing of strategic information (typologies, trends) in order to enhance the understanding of money laundering and terrorist financing (ML/TF) risks
- Improve the quality of suspicious transaction and activity reporting by obliged entities
- Preparation of risk indicators and red flags in order to improve the detection by private sector entities of suspicious financial flows

- Work on risk mitigation measures related to specific money laundering and terrorist financing (ML/TF) risks
- Joint capacity building/training activities and provision of technical assistance
- Other

**Please elaborate on your answer to question 11:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe all matters raised above are highly important and should be included in the objectives to be achieved by a PPP. However, we encourage the EC to provide further clarity what these objectives would entail in practice and how to apply them in the context of different sectors and professions. In our reply, we reflect on these issues from the perspective of the accountancy profession and in the context of services it provides.

#### General observations

Some of the points listed can be considered as objectives and others as outcomes. For example, the STRs /SARs quality will improve if there is better information sharing and better understanding of the red flags. This will lead to better STs identification and reporting. Given that 'strategic information-sharing' on trends and typologies is closely linked to the STRs/SARs quality, they should not be considered as separate objectives.

We refer to a Dutch example of intelligence-sharing to illustrate that the focus should be on quality of information rather than the quantity of the red flags raised. The national transaction data sharing system in the Netherlands (Transaction Monitoring Netherlands) indicated that sharing intelligence by using algorithms can facilitate the speed and increase the quality and relevance of the data. Nevertheless, despite the benefits that digitalisation can offer, what remains key is to ensure that the information shared on STs is targeted and enhances the understanding of money laundering and terrorist financing.

#### Sharing of strategic information

The EC should provide clarity what type of strategic information PPPs should encompass. If the purpose is sharing information based on the analysis of large sets of transactional data, this objective would not be applicable in the context of the accountancy profession.

In this respect, large financial institutions with access to data analytics may have capacity for more advanced information sharing. The accountancy profession due to the nature of their services can contribute with typologies and red flags. However, compared to financial institutions they often do not have an ability to see the immediate money laundering asset flows in action, but rather pick it up at a later stage.

#### Joint capacity building

We generally see joint capacity building as a positive objective to achieve. Further clarity is needed on what this joint capacity building would entail in practice and how it would apply in the context of different sectors and entities. We do not believe a 'one-size-fits-all' model will be an optimal solution due to the variety of sectors involved in the AML ecosystem with their specific activities and skillsets. We encourage the EC to consider several models how joint capacity building could operate for different sectors and entities.

For example, if this capacity is intended to be built through sharing specific data that would facilitate criminal networks mapping, the DNFBPs such as the accountancy profession would not have access to such data.

However, if the purpose is to develop a collaborative network, where participants exchange on trends, typologies, risk indicators the profession can bring useful input to the discussion. In addition, the profession can usefully contribute to joint capacity building through training activities and provide technical assistance in certain areas.

Therefore, the PPP model needs to be sufficiently flexible to be effective. We would welcome the opportunity to discuss with the EC how the accountancy profession's skills, knowledge, expertise and information could be leveraged to better fight economic crime.

---

**Question 12. Based on your experience, what impact (if any) do public-private partnerships for the exchange of strategic information have in the prevention of and fight against money laundering and terrorist financing and how significant is it?**

- Very positive effect
- Some positive effect
- Neutral
- Some negative effect
- Very negative effect
- Don't know / no opinion / not applicable

**Please explain your answer to question 12 and give examples:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In our experience PPPs can have a very positive effect for the exchange of strategic information if they work well. To this end, the PPPs need to be well designed, structured, and targeted to ensure that all relevant sectors are considered.

There are some good examples of PPP collaboration in the banking sector. For instance, Dutch law enforcement saw promising results in data sharing based on algorithm analysis (cf. the Dutch example quoted under question 11). However, we would like to observe that in most cases PPPs are largely structured around the larger banks' activities without consideration of other obliged entities' specific features.

Strategic information exchanged in the PPP setting needs to be applicable and relevant for the respective sector. For example, the exchange of strategic information on money mules can be highly useful for some sectors while completely irrelevant for others. Therefore, there should not be just one PPP model for strategic information exchange to have a real impact. The PPP model needs to be flexible to accommodate specificities of all actors concerned.

**Question 13. Where do you see risks stemming from the exchange of information in a public-private partnership for the exchange of strategic information in the context of preventing and fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Profiling with regard to specific persons or groups of persons
- Official secrecy and the disclosure of sensitive non-public information
- Bank secrecy
- Legal privilege

- Social and economic inclusion (e.g. de-risking and reputational risks)
- Other

**Please specify to what other risk(s) you refer in your answer to question 13:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Under the option 'other', we see two additional potential perception risks stemming from participation in a PPP. The first risk relates to how clients would perceive their advisers' (e.g. their accountant) participation in a PPP i.e. they may have concerns when specific data is shared. This could lead clients being less open with their advisers. This risk could also be relevant at an operational level. The second risk relates to supervisors' perception i.e. they may consider that those who do not participate in a PPP are somehow "failing". We believe that participation should remain voluntary, especially when firms are small.

**Please elaborate further on your answer to question 13:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

All listed options can be considered as potential risks. We selected the two options above as we believe that these are the key risks stemming from the exchange of strategic information in a PPP. Issues such as reputational risks, profiling, social and economic exclusion can entail adverse consequences for some individuals when certain strategic information is shared e.g. exclusion from financial or accounting services.

We believe that the other risks mentioned such as official secrecy, bank secrecy and legal privilege are indeed potential risks. Nevertheless, a proper legal framework can address these types of risks through appropriate control mechanisms.

**Question 14. In your opinion, in relation to the application of which rules is the issuing of guidance with respect to public-private partnerships for the exchange of strategic information most needed?**

Please select as many answers as you like

- Provision of feedback on suspicious transaction reports by the FIU to the obliged entity
- Fundamental rights (e.g. data protection, privacy)
- Antitrust rules (e.g. to avoid asymmetries of information)
- Other

**Please elaborate further on your answer to question 14:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

#### Provision of feedback on STRs by the FIU to the obliged entity

We recommend the EC takes a broader perspective on the purpose of the PPPs. PPPs should be a forum to exchange on trends, typologies pooled out from the STRs and processed into more practicable insights, developments and strategic matters.

We are not convinced that PPPs are the right setting for the provision of feedback on STRs by the FIU to the obliged entity. This process is resource intensive and would not directly contribute to the key PPP objectives such as promoting collaboration and information exchange. However, the EC guidance on FIUs' feedback on STRs quality would be useful. Similarly, generic feedback by FIUs on red flags with specific examples of common errors or mistakes would also be of benefit to obliged entities.

As a separate point, supervisor need to be informed of potential deficiencies in the STRs quality in order to increase effectiveness of the reporting regime.

#### Safeguarding fundamental rights, privacy and data protection

We believe that indeed safeguarding fundamental rights, privacy, data protection, protection against defamation and access to basic services are the key areas where guidance will be needed. This will be important to ensure the exchange of strategic information is balanced. We also agree that guidance in the area of antitrust rules linked to the competition law is needed.

Duty of confidentiality and security clearance to receive the information are additional areas linked to data protection which require further EC guidance and can be added to the list above. We believe these aspects are highly relevant in facilitating PPPs.

#### More clarity on the application of the GDPR

There is a need for more clarity on the application of the GDPR in the context of the AML legislation and in particular with respect to PPPs for the exchange of strategic information. AML and CFT rules encourage to gather and analyse as much data as possible to identify patterns and criminals, whereas the GDPR aims to restrict the use of personal data on a large scale. This can create potential conflicts of interest.

Furthermore, OEs in financial and non-financial sector have pointed to the need for additional rules to facilitate data use and exchange. Currently, data exchange is limited due to different interpretations of the GDPR. Data protection authorities need to provide a clear guidance to ensure that data protection rules do not inadvertently prevent information exchange or making use of technology.

The rules should be suitable for balancing key issues such as the relationship between the duty of confidentiality and data protection and the AML/CFT duties. This should apply on an equal basis to all parties that are subject to a duty of confidentiality.

## IV. Public-private partnerships for the exchange of operational information and intelligence on suspects in a criminal investigation and/or persons of interest prior to the opening of a formal criminal investigation

---

**Question 15. In your opinion, what should be the main objectives of a public-private partnership for the exchange of operational information in the context of fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Obtaining leads in the context of criminal investigations, based on the sharing of operational information by competent authorities
- Obtaining evidence as regards suspects in criminal investigations based on operational information shared by competent authorities
- Monitoring the transactions of suspects in criminal investigations
- Identifying persons of interest prior to the initiation of a formal criminal investigation by the competent authorities
- Monitoring the transactions of persons of interest prior to the initiation of a formal criminal investigation
- Mapping criminal networks, based on the sharing of operational information by competent authorities
- Other

**Please elaborate on your answer to question 15:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In principle all these actions will be crucial to prevent individuals from planning and engaging in illegal transactions such as engaging professionals to assist in their operations, setting up vehicles to enable these operations and prevent the lack of transparency.

However, we see these objectives of specific relevance at the top end of major financial institutions. We are not convinced they are applicable for all sectors and in particular the accountancy profession.

The concept of 'operational information' itself is difficult to apply in the context of the accountancy profession. The profession will not be able to map criminal networks based on transaction records as it is not working with transactions. However, the profession can help map criminal activity or criminals' 'journey' throughout the financial system, which can help to better recognise red flags. Therefore, we recommend the EC reflects on the PPPs' objectives with better consideration for the specificities of different sectors involved.

In addition, we would like to observe that the listed points would benefit from a better structure. Some of them should be the PPPs' objectives while others follow-up actions for law enforcement to take forward as an operational matter. For example, identifying persons of interest and mapping criminal networks are elements of intelligence sharing. Once this information is shared, obtaining leads, evidence and monitoring are follow up actions for law enforcement.

Therefore, we recommend making a distinction between them e.g. as stage 1 and stage 2 to ensure more focus and clarity.

**Question 16. Based on your experience, what impact (if any) do public-private partnerships for the exchange of operational information have in the fight against money laundering and how significant is it?**

- Very positive effect
- Some positive effect
- Neutral
- Some negative effect
- Very negative effect
- Don't know / no opinion / not applicable

**Please explain your answer to question 16 and give examples:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The accountancy sector has limited experience in this area. However, there are indications that this information has the potential of becoming increasingly useful.

**Question 17. Based on your experience, what impact (if any) do public-private partnerships for the exchange of operational information have in the fight against the financing of terrorism and how significant is it?**

- Very positive effect
- Some positive effect
- Neutral
- Some negative effect
- Very negative effect
- Don't know / no opinion / not applicable

**Please explain your answer to question 17 and give examples:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The accountancy sector does not have direct experience in this area. We understand that in the banking sector the effect is very positive. Such information exchange would usually take place post factum and allow identification of criminal network. To add, sharing operational information to fight the financing of terrorism seems more challenging because it requires intelligence on suspects.

**Question 18. Where do you see risks from the exchange of information in a public-private partnership for the exchange of operational information in the context of fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Fundamental rights (rights to the protection of personal data and privacy, the presumption of innocence)
- The integrity of ongoing criminal proceedings
- Official secrecy and the disclosure of sensitive information related to ongoing criminal proceedings
- Bank secrecy
- Legal privilege
- Social and economic inclusion (e.g. de-risking and reputational risks)
- Other

**Please elaborate further on your answer to question 18:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We see safeguarding fundamental rights such as the protection of personal data and privacy, the presumption of innocence as key risks from the exchange of operational information in a PPP. Regulators need to ensure that individuals or entities are not subject to significant consequences without the opportunity to put their case to appropriate legal oversight or scrutiny. Similarly, we believe that social and economic inclusion is a risk as it can entail adverse consequences for some individuals when certain operational information is shared e.g. names or other details.

Apart from the selected choices, we note that risks exist also on a horizontal level when clients appear to have closer relationship with the obliged entity. In these cases, information leaks become highly probable.

Any PPPs should include provisions to ensure that legal privilege is protected in the interest of the criminal justice system. There can be also other cases where it is inappropriate to share information.

As discussed in our reply to question 13, for matters such as official secrecy, bank secrecy and legal privilege, we believe a proper legal framework can manage these types of risks through appropriate control mechanisms.

**Question 19. In your opinion, in relation to the application of which rules is the issuing of guidance with respect to public-private partnerships for the exchange of operational information most needed?**

Please select as many answers as you like

- Fundamental rights (e.g. data protection, privacy, presumption of innocence)
- The applicable criminal procedural rules
- Antitrust rules
- Other

**Please elaborate further on your answer to question 19:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe the guidance will be needed in the areas of protection of fundamental rights and antitrust rules e. g. examples of sector characteristics, markets, products, etc. that are more vulnerable for non-compliance with antitrust regulations.

The exchange of operational information needs to be voluntary. It is critical to provide further clarifications on which information can be shared, used, stored and to ensure the necessary protections are in place.

Personal safety should be considered especially in cases where small organisations are involved in PPPs. In addition, it will be useful to provide guidance on the conditions of participation and security screening and how the data is used.

**Question 20. Are you of the opinion that the risks from the exchange of information in a public-private partnership for the exchange of operational information are different in the context of fighting money laundering than in a public-private partnership in the context of fighting the financing of terrorism?**

- Yes
- No
- Don't know / no opinion / not applicable

**Please elaborate further on your answer to question 20:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We do not believe there are substantial differences when it comes to risks stemming from the exchange of operational information in PPPs to fight money laundering or terrorism financing. We believe nevertheless that sharing operational information to fight terrorism financing is more challenging because this requires intelligence on suspects or persons of interest.

## V. Transnational public-private partnerships

---

**Question 21. In your opinion, what information can be shared in a transnational public private partnership in the framework of preventing and fighting money laundering and the financing of terrorism?**

- Strategic information (typologies, trends, patterns, risk indicators)
- Operational information (intelligence on suspects or persons of interest)
- Both types of information
- Other

**Please elaborate further on your answer to question 21:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Both types of information could be shared provided there are clear legal pathways. Sharing information also requires confidence on the part of the sharing organisation that appropriate controls (appropriate legal framework and clear oversight) have been put in place in other Member States. This point is particularly relevant for the situations where there are divergent approaches to data privacy and protection across jurisdictions. This can cause concerns how certain strategic or operational information might be used.

Finally, there also needs to be the Member States' willingness to collaborate.

**Question 22. In your opinion, what are the main potential benefits of establishing a transnational public-private partnership in the framework of preventing and fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Better understanding of the cross-border risks associated with money laundering and the financing of terrorism
- More effective detection of cross-border suspicious financial flows by private sector entities
- More effective cross-border financial investigations into money laundering and the financing of terrorism
- Other

**Please specify to what other main potential benefit(s) you refer in your answer to question 22:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Transnational PPPs can also enhance obliged entities' understanding of the differences in cross border activities related to institutions, legal structures, processes and procedures. This insight is highly relevant for the work with international clients.

## **Please elaborate further on your answer to question 22:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe all the above could be potential benefits provided there is a good framework. Money laundering knows no borders; hence, introducing restrictions on such partnerships impedes bringing down criminal networks. This collaboration needs to happen within a safe and secure context.

There is an interest for the accountancy profession to be able to share pertinent information across countries to better fight money laundering and to alert other firms on potential money laundering threats. Currently such exchanges can happen only in a very restrictive manner, which is a challenge.

## **Question 23. Where do you see risks stemming from the exchange of information in a transnational public-private partnership in the context of preventing and fighting money laundering and the financing of terrorism?**

Please select as many answers as you like

- Rights to the protection of personal data and privacy
- Fundamental rights, including the presumption of innocence
- The integrity of ongoing criminal proceedings
- Official secrecy and the disclosure of sensitive information related to ongoing criminal proceedings
- Bank secrecy
- Legal privilege
- Social and economic inclusion (e.g. de-risking and reputational risks)
- Other

## **Please elaborate further on your answer to question 23:**

*5000 character(s) maximum*

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In all the above cases, there can be risks involved. There are likely to be additional complications for the exchange of information in the transnational PPP due to differences in legal and supervisory structures as well as protections. For example, even in the EU there are different interpretations of the AML rules. Indicatively, not all legal systems are based on the principle of presuming innocence until proven guilty.

We refer to our replies under questions 13 and 18 which are also relevant for the exchange of information in the transnational PPP.

## Additional information

---

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) below. **Please make sure you do not include any personal data in the file you upload if you want to remain anonymous.**

The maximum file size is 1 MB.

You can upload several files.

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

**5f2f6f29-22d7-4613-96af-20a7b7d7f4f0/Annex\_to\_Question\_2\_-\_EC\_consultation\_on\_PPPs.pdf**  
**27a796f0-571b-4be6-86b9-e96e3b6847b5/Building-an-effective-AML-ecosystem.pdf**  
**ab25b08e-cd14-436e-b23b-dec8cffbba63/Building-an-effective-Anti-Money-Laundering-ecosystem-summary.pdf**

### Useful links

[More on this consultation \(https://ec.europa.eu/info/publications/finance-consultations-2021-anti-money-laundering-public-private-partnerships\\_en\)](https://ec.europa.eu/info/publications/finance-consultations-2021-anti-money-laundering-public-private-partnerships_en)

[Consultation document \(https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-document\\_en\)](https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-document_en)

[Consultation strategy \(https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-strategy\\_en\)](https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-strategy_en)

[More on anti-money laundering and countering the financing of terrorism \(https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism\\_en\)](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en)

[Privacy statement \(https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement\)](https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement)

[More on the Transparency register \(http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en\)](http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en)

### Contact

fisma-financial-crime@ec.europa.eu

