Contribution ID: be3f8bb5-935f-4bf4-8024-d7ad1028f772
Date: 01/11/2021 17:19:25

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) (https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en). 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 (https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en) 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 4th Anti-Money Laundering Directive (https://ec.europa.eu/info/law/anti-money-laundering-amld-iv-directive-eu-2015-849_en)) 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) (https://edpb.europa.eu/edpb_en) 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 (https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how_en), 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 (https://ec.europa.eu/info/publications/finance-consultations-2021-anti-money-laundering-public-private-partnerships_en)
- the consultation document (https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-document_en)
- the consultation strategy (https://ec.europa.eu/info/files/2021-anti-money-laundering-public-private-partnerships-consultation-strategy_en)
- 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)

- on the protection of personal data regime for this consultation (https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement)

About you

*Language of my contribution

English

*I am giving my contribution as

Non-governmental organisation (NGO)

*First name

Michele

*Surname

Sciurba

*Email (this won't be published)

sciurba@gmvv.eu

*Organisation name

255 character(s) maximum

Strategic Think Tank GMVV & Co. GmbH

*Organisation size

Small (10 to 49 employees)

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register (http://ec.europa.eu/transparencyregister/public/homePage.do?redir=false&locale=en). It's a voluntary database for organisations seeking to influence EU decision-making.

Transparency Register Public ID 117389937064-08

*Country of origin

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

Germany

*Field of activity or sector (if applicable)

- [ ] Accounting
- [ ] Art dealing
- [ ] Auditing
- [ ] Banking
- [ ] Company and trust creation and management
- [x] 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
- [x] 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 (https://ec.europa.eu/info/law/better-regulation/specific-privacy-statement)

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?

5,000 character(s) maximum

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

Based on the experience with companies such as World-Check, the transfer of sovereign tasks to private companies must be rejected for the following reasons. The contribution that these companies make to combating money laundering (AML) and terrorist financing (CTF) is neither statistically recorded nor transparent. In contrast, many significant fundamental rights violations of EU citizens have been documented and proven by unjustified entries in databases such as World-Check.

Privatized warning and black lists from databases like World-Check are highly problematic, since they include individuals who have never been convicted of a crime or subject to official investigations. Those affected may be denied bank accounts or refused transactions. Despite these severe repercussions, there are no procedures to get de-listed from World-Check. Privatized databases like World-Check include only publicly available data and hence claim no responsibility of their content, referring complaints to their sources such as the investigating authorities. It is unclear to what extent this practice constitutes a breach of rights to privacy, especially with regard to the new General Data Protection Regulation (GDPR). Due to the lack of clarity about privacy and legal remedies, the privatization of terrorist lists is insufficiently accountable to constitutional principles such as the presumption of innocence and due process.

World-Check was established in 2000 and belongs to the American group Refinitiv; 45% of Refinitiv's shares are owned by Thomson Reuters and 55% by the American Blackstone Group LP, the largest independent asset manager in the world. World-Check provides its clients with records on individuals and legal entities (including organizations), namely politically exposed persons (PEP), their family members and close associates. Information of listed persons includes connections to third parties as well as informal sources, such as media reports, mentioning the persons or relating them to keywords such as "political", "corporate", "military", "crime/drugs" and "terrorism". By 2014, World-Check had presumably listed 2.2 million data records. Currently, customers can access more than 3 million data records ad hoc and link them to their own data processing systems to maintain blacklists of undesirable business relationships tailored to their own needs. According to World-Check, 40,000 new profiles are added each month and 80,000 profiles are updated with information on address data and other personal data. Users include more than 6,000 customers in 170 countries, including 49 of the 50 largest banks, 9 of the 10 largest law firms and more than 300 government organizations and intelligence agencies (secret services).

For those affected who end up on the World-Check lists or other privatized terror lists, these lists do not as yet offer procedures for de-listing. By contrast, the UN has introduced an ombudsman procedure for the de-listing of individuals under Security Council Resolution 1904 (2009). As a response to criticism about the lack of fair proceedings, those affected can now request the de-listing from the ISIL and Al-Qaeda sanction lists, the main lists from the currently 13 UN sanction lists. This shows that the present system of compiling and maintaining private terrorist lists is deeply flawed because it offers no legal recourse to those wrongly suspected of terrorist activity and is not subject to democratic scrutiny.

Today, an entire industry specializes in providing credit institutions with the data necessary for customer due diligence on a regular basis. In doing so, the financial industry receives data from thousands of sources and databases for its research and monitoring systems. For the customers of financial institutions, however, this process lacks transparency with regard to the data used for the customers' "risk classification". In addition, the globalized and increasingly complex due diligence system escapes transparent

democratic and constitutional control. Especially within the EU, where the GDPR aims to achieve a high level of protection for personal data and its use by third parties. The established data protection practice strongly contradicts the AML/CTF legislation. Affected individuals have no insight into what data is being accessed nor can they understand what they are used for.
The compatibility of the EU Money Laundering Directives with the EU Charter is de facto no longer given. Yet, the 4th AML Directive 2015/849 states at (65): "This Directive respects the fundamental rights and observes the principles recognised by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence."

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:

5,000 character(s) maximum

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

Today, an entire industry specializes in providing credit institutions with data for customer due diligence and the financial industry receives data from thousands of sources and databases for research and monitoring (Schufa, ClariLab, World-Check, etc.). For customers whose data is the target of such reporting, the process is highly problematic, in part because of the criteria used to determine customers' 'risk classification'. Those individuals affected have no insight into what data is being accessed or the use to which it is being put. In addition, there are few legal or constitutional checks on this globalized and increasingly complex due diligence system. In the EU, especially with the introduction of the General Data Protection Regulation (GDPR), which requires a high level of protection for personal data and its use by third parties, data protection law contradicts the compliance requirements prescribed by AML/CTF legislation.

From a German view, the de-risking policy practiced by banks leads to unintentional discrimination, for instance by the bank refusing to open bank accounts for people with migrant backgrounds or other factors the bank classifies as "risk-increasing". Thus, individuals are discriminated against solely because of their origin and are excluded from a wide range of financial services.

The case law of the Federal Constitutional Court in the Federal Republic of Germany recognizes that the freedom of contract between private parties must be brought into line with Article 3(1) of the German Constitutional Law (GG) if the effect of the principle of equal treatment is disturbed by the fact that an offer under private law, which is open to a large public without regard to the person and which determines participation in social life to a considerable extent for the persons concerned, is not available to certain interested parties. The use of databases can not only lead to, but is even intended to deprive – in private legal, service and economic transactions the persons or organizations listed on World-Check and other private databases – from financial services. The exclusion of those persons or organizations listed, according to established German legal understanding, are assigned to the protection area of the core area of general freedom of action under Art. 2(1) GG.

At the supranational level, too, the protection of equality and from discrimination under EU law, which is reflected in the EU Charter of Fundamental Rights' catalog cannot be reconciled with the already existing practice of using private database services, which in the financial sector leads to the exclusion of entire population groups from certain financial services. The three-layered equality regime in the EU begins with Article 18(1) TFEU, which is followed by the more specific prohibitions of discrimination and restrictions of fundamental freedoms in Articles 34, 45, 49 and 56 TFEU.

These transnational integration norms serve primarily to protect against unequal treatment because of different nationalities. These protections are primarily intended to have a market-integrating function. The counterbalance to this are the equality guarantees of the EU Charter of Fundamental Rights' Art. 20, 21, 23 and 26. The guarantees and prohibitions of discrimination, which are intended to ensure non-discriminatory participation in social, political and economic life in the EU, are also supported by Art. 14 of the European Convention on Human Rights (ECHR), which ensures non-discriminatory protection of the rights enshrined in the Convention and thus constitutes an accessory prohibition of discrimination (cf. Münch/Kunig, GG Kommentar (7th edn) 212). In addition, Art. 1 of the 12th Additional Protocol to the ECHR contains a general prohibition of discrimination.

Public-private partnerships (PPPs) lead to a lack of democratic controls and

thus a lack of democratic legitimacy. There is a great lack of transparency and clear procedures to protect people from arbitrary entries in private databases such as World-Check. In addition, there is a lack of EU-wide legal remedies to ensure a due process of law so that people can defend themselves against entries in databases like World-Check.

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?

5,000 character(s) maximum

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

The 4th AMLD has expanded both the range and targets of predicate offenses for money laundering, including tax crimes. EU legislation grants investigative authorities such extensive powers that no reasonable grounds for suspicion are necessary to become the subject of an investigation. The 4th AMLD requires not only credit and financial institutions but also lawyers, trustees, company service providers, real estate agents and gambling companies to carry out customer due diligence and to report suspicious transactions to the competent authorities. Thus, the 4th AMLD not only compromises the fiduciary relationships between banks and their customers but also the confidentiality requirements of tax advisors, lawyers and others. In particular, the 4th AMLD's severe sanctions regime for the non-reporting of suspicious transactions, the lack of a definition of 'suspicious transactions' and the lack of sanctions for over-reporting suspicious financial activities undermine privileged attorney-client relationships. As a result, citizens can no longer trust that advisors protect privileged relationships, but must assume they will be reported to the authorities even in the absence of reasonable grounds for suspicion because of the fear of running afoul of compliance regulations. Employees of financial institutions, and now lawyers and tax advisors, have been involuntarily drafted into the role of policing the AML regime in the EU and the FATF states. This raises basic problems of competence and the fair application and enforcement of the rule of law.

Currently, AML legislation in most jurisdictions worldwide, for example the Indian Prevention of Money Laundering Act 2002 and the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006, have created a legal obligation of cooperation between many "obligated parties" under the 4th AMLD, which is equivalent to an involuntary PPP. Moreover, institutions, tax advisors, lawyers and others are subject to the risk of considerable sanctions if they do not apply a sufficient compliance structure in line with AML/CTF legislation.

A cost-benefit analysis of AML/CTF legislation raises significant questions about the economics of regulation. In 2014, 15 enforcement agencies recovered only £ 155,000,000 in criminal proceeds while spending an estimated £ 100,000,000 on administrative costs. The British Bankers' Association estimates that the largest international banks spend £ 700,000,000 to £ 1,000,000,000 annually on financial crime compliance. AML/CTF legislation involves significant regulatory, financial and personnel costs without yielding proportionate social and economic benefits. This is also true with respect to the effectiveness of AML/CTF measures in preventing terrorist attacks. In its 2016 recommendations on terrorist financing, the FATF states that monitoring financial flows, including cash transactions, helps the investigators to identify terrorists and prevent terrorist attacks. However, upon closer inspection, the implementation of the FATF Recommendations has been more effective in uncovering cases of minor tax evasion than preventing terrorist attacks. In recent years, only minimum financial resources are needed to carry out terrorist attacks. The Nice attack of 14 July 2016, in which ISIS fanatic Mohamed Lahouaiej-Bouhlel killed 86 people and injured more than 450 others with a cargo truck, cost no more than £ 2,200, according to the estimates of the Center for the Analysis of Terrorism (CAT). This latest low-tech strategy for terrorist attacks is based on the use of ordinary objects and vehicles as weapons. The London attack on 22 March 2017 at the Westminster Bridge, which killed three people and injured 20 others, and the Berlin Christmas Market attack on 19 December 2016, where 12 people were killed and around 50 others were injured, were carried out using improvised weapons such as vehicles and knives. Overall, the catch-all

approach of the AML/CTF regulations is portrayed politically and in the media as a proven means of preventing terrorism, but it is ill-suited to prevent low-tech terrorist attacks, since they are cheap and materialize quickly. Most terrorist attacks in recent years have not required major financial transactions or big sums of money. Yet, the policy makers and investigative authorities continue to insist that the expansion of AML/CTF legislation worldwide is necessary.

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 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

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

5,000 character(s) maximum

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

The 4th AMLD raises significant questions about the adherence of fundamental principles of the law and the rights of defendants. While EU Member States usually harmonize criminal law from the bottom up, European AMLDs have established top-down measures against money laundering to accelerate European harmonization. Nevertheless, there remain major differences among Member States in the implementation of the Directives, especially with regard to predicate offences for money laundering. Money laundering by international organized crime is a concern of both the EU and the international community and has prompted closer cooperation among nation states at the legislative, executive and judicial levels. The 1998 European Joint Action Plan established cross-border cooperation to fight organized crime. The creation of the European center Eurojust, which coordinates judicial cooperation between the national law enforcement agencies, has been a crucial step in the fight against organized crime and money laundering within the EU. The establishment in 2009 of the European-wide police force and independent international organisation Europol was a further step in combating cross-border crime.

In 2013, the EU Commission developed a proposal to further improve Europol and Eurojust, respectively. In 2016, based on the Europol proposal, the EU adopted a regulation that defines Europol's operation within the EU with regard to cross-border cooperation and criminal matters in detail. A similar regulation was adopted in 2018 for Eurojust – Regulation 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust) – following the establishment of the European Public Prosecutor's Office by Regulation 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'). The responsibility of the European Prosecutor includes the prosecution of serious cross-border crimes and criminal cases involving illegal activities that affect the financial interests of the EU according to Article 325 TFEU. The national courts of the Member States, however, are in charge of accusations and indictments.

The establishment of a European law enforcement authority has fundamentally changed judicial cooperation within the EU, as this authority can initiate independent investigations in the participating EU Member States. It is evident from the Encro-Chat investigations that EU law enforcement agencies such as Europol and Eurojust lack democratic scrutiny and monitoring that ensure the observance of fundamental rights. The political and legal challenge for the EU and its Member States is to hold onto fundamental rights of due process and constitutional guarantees by not subordinating them to the fight against crime. At the moment, it shows that the procedures of Eurojust, Europol and the investigative authorities of the Member States in connection with the Encro-Chat investigations have fully ignored transparency and democratic and judicial safeguards. As a result, hundreds of wiretappings took place in various Member States without prior judicial orders and appropriate judicial review.

At the level of Eurojust, "confidentiality" is implemented by the legal requirements; cf. Regulation 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust), Article 72. There is, in principle, nothing wrong with investigative authorities investigating wrongdoing and criminal acts in a coordinated manner at the European level; however, international legal standards require that these investigative acts and methods must be reviewable in a procedure based on the rule of law while respecting the rights of the accused. However, this is currently not guaranteed. The classification as "confidential" prevents the verifiability of data, which is diametrically opposed to the principles of the rule of law.

This lack of democratic safeguards is further exacerbated by the expansion of PPPs. In the process, the ever-increasing cooperation with private actors such as World-Check, etc., leads to a boundless surveillance of citizens that can no longer be democratically controlled and legitimized. It is not clear whether the EPPO will improve the prosecution of serious crimes within the EU. There are a lot of issues to resolve, including the absence of full legal harmonization within the Union, the question of how to accommodate different criminal regulations in Member States and the need for defining legal remedies vis-á-vis a European Public Prosecutor. Measures to ensure democratic scrutiny of the process will be of central importance for the fairness of criminal proceedings handled by the EPPO, Europol, and Eurojust.

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

- [x] Financial institutions
- [x] Credit institutions
- [x] 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:

5,000 character(s) maximum

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

The 4th AMLD raises several questions about the absence of democratic and legal safeguards for protecting the privacy of EU citizens. It needs to be examined whether the obligation of financial, economic and legal actors – such as financial and non-financial institutions and their employees and all other obligated parties, such as tax advisors, lawyers, trustees – under the 4th AMLD for preventive and repressive cooperation in the fight against money laundering and terrorist financing and the implementation of the EU AMLDs in national law is permissible. The example of the private market leader database "World-Check", which is offered under private law, shows that the obligation of private parties to combat cross-border money laundering in accordance with EU money laundering directives is in principle compatible with the protection of the fundamental rights of those affected, also regarding data protection law. However, the paradigm shift, which since the 4th AMLD has led to a systematic transfer of sovereign investigative tasks to the obligated parties under the Directive, constitutes an inadmissible restriction of the core area of German criminal procedural law under German federal constitutional law.
While the 4th AMLD was passed as a provision of EU administrative law to fall within the competence of the EU, in fact the Directive is a matter of criminal law. As a result, the provisions of the latest version of the Money Laundering Act (GWG 2017), which was rewritten to implement the 4th AMLD in German law, disproportionately interfere with the rights of those affected and those obligated. The EU must take greater care by implementing stronger democratic control mechanisms to prevent the transformation of the civil state under the rule of law into a comprehensive surveillance state through the disproportionate implementation of the EU Anti-Money Laundering Directives with covert de facto criminal procedure provisions.

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?

5,000 character(s) maximum

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

For their own protection, banks are now reporting customers at an early stage on suspicion of money laundering. The indications of suspicion are often completely arbitrary; actual evidence of misconduct is rare, as can be statistically proven. In R v GH [2015], the UK Supreme Court pointed out another problem with this EU AML legislation, which is unbridled in its vagueness, namely that prosecutors are improperly using charges such as money laundering to significantly expand the prosecution's scope of action against the accused. The risk-based approach to financial crime called for by the 4th AMLD requires banks to assess their customers on factors such as:

- Sector, profession, type of business activity
- Geographical and legal risk
- Political risk
- Distribution/supply channels
- Products or services that the customer needs or uses

In the absence of broadly defined and commonly used methodologies for assessing such risk factors, banks are expected to develop their own risk measurements. As noted by Professor Peter Reuter, co-author of the 2014 report "Global Surveillance of Dirty Money", which evaluates AML/CTF regulations, "the science of risk analysis is poorly developed for money laundering, and it is currently impossible to judge relative risk on an objective and systematic basis." As a result, banks cannot rely on sufficient data, but only on subjective assessment.
Since banks de facto are no investigative authorities that can assess "reasonable grounds for knowing and suspecting" as required by POCA 2002, the court ruled in K v National Westminster Bank [2006] that bank employees no longer have to meet legal requirements to file a money laundering report; instead, the bank employee's subjective feeling is sufficient to justify a report. Bank employees are also required in the EU to report to the authorities any suspicion of money laundering based solely on a subjective feeling, which led to a massive increase in such reports in the EU and the G20 countries. Even in Switzerland, the number of SARs filed by banks increased from 619 in 2006 to 4,125 in 2018, and the situation is similar in Germany, where the number of reported SARs increased from 2,997 in 2006 to 144,005 in 2020. In the UK, a total of 318,445 SARs were received between October 2014 and September 2015, of which 83.39% were from the banking sector. These figures show that the principles of the rule of law are being eroded in favor of a seemingly better fight against crime.

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:

5,000 character(s) maximum

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

Within the EU, government FIUs share data among themselves. Internationally, the extent and parameters of data exchange among FIUs is regulated through data exchange agreements. This exchange of data is not only far-reaching, but it takes place largely without the knowledge of those affected. In 2015, 151 FIUs, members of the Egmont Group, exchanged data based on the Interpretative Note 29 of the FATF Recommendations, which states: "In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data."
Interpretative Note 29 illustrates a breath of data exchange between FIUs and law enforcement agencies that largely eludes democratic control or constitutional scrutiny. The decisions of the ECJ in recent years have allowed massive intrusions into fundamental freedoms and human rights by defining the fight against money laundering and the associated AML legislation as a "general interest" of the Union, and this rationale has been used to limit the application of the ECHR. The European Court of Human Rights (ECtHR) has reached a similar judgement.
These decisions by the ECJ and ECtHR are difficult to comprehend, as both the FATF and FIUs have not produced any statistics or evidence-based research that would prove that the 40+9 FATF Recommendations have led to fewer terrorist attacks. There is no statistical evidence that the immense cost to the private sector of complying with AML/CTF provisions results in less money laundering. However, there is clear evidence of the immense unintentional discrimination caused by AML/CTF provisions, as well as the lack of transparency and the dismantling of rule-of-law guarantees. A much stronger involvement of NGOs such as Fair Trials International, Human Rights Watch or Transparency International would provide a counterweight to the increasingly strong asymmetry between the fight against crime and the protection of fundamental rights.

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

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
- [x] 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:

5,000 character(s) maximum

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

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:

5,000 character(s) maximum

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

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

- [x] Profiling with regard to specific persons or groups of persons
- [ ] Official secrecy and the disclosure of sensitive non-public information
- [x] Bank secrecy
- [x] Legal privilege
- [x] Social and economic inclusion (e.g. de-risking and reputational risks)
- [ ] Other

Please elaborate further on your answer to question 13:

5,000 character(s) maximum

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

Sanctions against financial institutions that violate their obligations under current AML/CTF legislation has led financial institutions to implement comprehensive "de-risking" measures. Financial institutions have implemented systems to identify and close potential "at-risk" accounts held by certain groups of customers or prevent them from opening accounts in the first place. Financial institutions today terminate customer accounts for money transfers, currency exchanges, check cashing, or the transfer or receipt of funds from or to certain geographic "risk regions", such as Turkey, Middle Eastern countries, Russia, or Ukraine, just to minimize their own risk of being sanctioned. One factor in the risk assessment of financial institutions is the cost of maintaining correspondent banking relationships, as AML legislation requires them to know not only the customers, but also the customers' customers (KYCC). As a result, it is almost impossible to conduct financial transactions with "at-risk" regions. This financial exclusion due to "de-risking" has resulted in 2.5 billion adults (41% of adults) in developing countries not currently having access to a bank account. In developed economies, nearly 90% of adults have a bank account at a formal financial institution. Financial exclusion in Europe today primarily affects people from immigrant backgrounds, particularly those of Muslim origin. Studies in the United Kingdom suggest that financial exclusion is due to rising Islamophobia.

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
- [x] 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:

5,000 character(s) maximum

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

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
- [x] Other

Please specify to what other main objective(s) you refer in your answer to question 15:

5,000 character(s) maximum

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

```
See answer 1.
```

Please elaborate on your answer to question 15:

5,000 character(s) maximum

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

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:

5,000 character(s) maximum

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

See answer 13.

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:

5,000 character(s) maximum

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

AML/CTF legislation involves significant regulatory, financial and personnel costs without yielding proportionate social and economic benefits. This is also true with respect to the effectiveness of AML/CTF measures in preventing terrorist attacks. In its 2016 recommendations on terrorist financing, the FATF states that monitoring financial flows, including cash transactions, helps the investigators to identify terrorists and prevent terrorist attacks. However, upon closer inspection, the implementation of the FATF Recommendations has been more effective in uncovering cases of minor tax evasion than preventing terrorist attacks. In recent years, only minimum financial resources are needed to carry out terrorist attacks. The Nice attack of 14 July 2016, in which ISIS fanatic Mohamed Lahouaiej-Bouhlel killed 86 people and injured more than 450 others with a cargo truck, cost no more than £ 2,200, according to the estimates of the Center for the Analysis of Terrorism (CAT). This latest low-tech strategy for terrorist attacks is based on the use of ordinary objects and vehicles as weapons. The London attack on 22 March 2017 at the Westminster Bridge, which killed three people and injured 20 others, and the Berlin Christmas Market attack on 19 December 2016, where 12 people were killed and around 50 others were injured, were carried out using improvised weapons such as vehicles and knives. Overall, the catch-all approach of the AML/CTF regulations is portrayed politically and in the media as a proven means of preventing terrorism, but it is ill-suited to prevent low-tech terrorist attacks, since they are cheap and materialize quickly. Most terrorist attacks in recent years have not required major financial transactions or big sums of money. Yet, the policy makers and investigative authorities continue to insist that the expansion of AML/CTF legislation worldwide is necessary.

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

- [x] 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
- [x] Bank secrecy
- [x] Legal privilege
- [x] Social and economic inclusion (e.g. de-risking and reputational risks)
- [ ] Other

Please elaborate further on your answer to question 18:

5,000 character(s) maximum

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

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

- [x] 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:

5,000 character(s) maximum

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

Considering the multitude of data exchange agreements between FIUs and third countries that lack democratic forms of government or have underdeveloped constitutional structures, the question is how the EU can ensure the legal guarantees under the Charter in practice. The exchange of data within the Egmont Group, the largest FIU cooperation network worldwide with over 150 members, is not only opaque but largely free of democratic controls. Since the Egmont Group includes not only countries like Germany, the UK, and Switzerland, but states like Saudi Arabia, Uzbekistan, and Sudan, it is completely unclear which guarantees the latter could give that complied with the Charter.
Over the past three decades, a far-reaching global system has been established to combat money laundering. The establishment of the FATF and the corresponding creation of international standards, which have been widely implemented, have promoted this system. Today, the FATF Recommendations have a significant impact on EU legislation. There are, however, considerable doubts as to whether these Recommendations are compatible with the rule of law, since the FATF is an 'ad hoc body' of countries that have disproportionately influenced the development of the FATF Recommendations. As a result, the process by which the Recommendations' criteria were created is not transparent. Ultimately, combining CTF and tax evasion prevention into the EU AML framework lumps together completely different phenomena making the whole system inefficient and legally questionable.

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:

5,000 character(s) maximum

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

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:

5,000 character(s) maximum

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

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
- [x] Other

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

5,000 character(s) maximum

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

Please elaborate further on your answer to question 22:

5,000 character(s) maximum

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

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

- [x] Rights to the protection of personal data and privacy
- [x] 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
- [x] Bank secrecy
- [x] Legal privilege
- [x] Social and economic inclusion (e.g. de-risking and reputational risks)
- [ ] Other

Please elaborate further on your answer to question 23:

5,000 character(s) maximum

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

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**.

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