Developing Public-Private Information Sharing to Strengthen the Fight Against Money Laundering and Terrorism Financing

Recommendations of the ISF-Police-funded Research Project "Public-Private Partnerships on Terrorism Financing" (ParTFin)

Benjamin Vogel, Maxime Lassalle

ABSTRACT

This article features the summary of the EU-funded ParTFin project. The full report can be downloaded below and separately cited by using a unique DOI number (10.30709/eucrim-2023-031). The project aimed at providing guidance for policymakers, competent authorities, and obliged entities on how to ensure that public-private information-sharing mechanisms in the field of financial crime can operate effectively and at the same time align with the Charter of Fundamental Rights of the European Union.

AUTHORS

Benjamin Vogel

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law (formerly Max Planck Institute for Foreign and International Criminal Law)

Maxime Lassalle

Maître de conférences
Université de Bourgogne

CITE THIS ARTICLE

Lassalle, M., & Vogel, B. (2024). Developing Public-Private Information Sharing to Strengthen the Fight Against Terrorism Financing and Money Laundering : Recommendations of the ISF-Police-funded Research Project "Public-Private Partnerships on Terrorism Financing" (ParTFin). Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-030

Published in eucrim 2023, Vol. 18(4) pp 384 – 392

https://eucrim.eu

ISSN:

I. Background

Recent years have seen an increase in public-private partnerships in the fight against financial crime. At the international level, such partnerships have been welcomed by the United Nations Security Council[1] and by the FATF.[2] At the EU level, partnerships are not only supported by a Commission Staff Working Document but have also been welcomed by the European Parliament and the Council during the ongoing negotiations on the anti-money laundering (AML) legislative package.[3] Meanwhile, a number of countries in and outside the EU have been developing partnerships of various design.[4] While most partnerships provide for an exchange of strategic information, some initiatives have already gone further and allow for the sharing of tactical information – that is, information that targets specific suspects and other specific persons of interest. The sharing of personal data is widely considered more problematic, however, as it affects fundamental rights more directly and is usually not provided for in national legal frameworks. These concerns were amplified in a letter by the European Data Protection Board.[5]

II. Purpose of the Recommendations and Methodology

The present Recommendations aim at situating public-private partnerships in the EU legal order and providing guidance for policymakers, authorities, and obliged entities on how to ensure that cooperation aligns with the imperatives of the Charter of Fundamental Rights of the European Union (CFR).

As a starting point, it should be stressed that public-private partnerships in anti-money laundering and countering the financing of terrorism (AML/CFT) can take many different forms. However, they typically involve the processing of customer data by obliged entities and, in order to induce or facilitate this processing, the provision of information to the obliged entities by authorities. Similarly, cooperation can emphasise different objectives – notably, the objective of improving the quality of obliged entities' customer due diligence (CDD) or the objective of advancing ongoing criminal investigations. Developing legal frameworks for public-private partnerships thus, in essence, means regulating the aforementioned forms of cooperation. In the process, the focus lies on those forms of cooperation that are most problematic from a fundamental-rights point of view, namely on practices that, in one way or another, target specific individuals, specific entities, or specific transactions.

In addition, discussions surrounding the topic of closer public-private cooperation in AML/CFT have so far been conducted chiefly under the umbrella of the term "partnership", denoting forms of cooperation that are voluntary. Yet it may sometimes, for practical or legal reasons, be desirable to create mechanisms for mandatory enhanced public-private cooperation. The present Recommendations therefore address new forms of cooperation more broadly, whether they are voluntary or not.

On a last note on the objectives pursued by the Recommendations, it is worth underlining that the Recommendations are marked by the desire to find an appropriate balance between the conflicting interests at stake: strengthening the fight against financial crime while at the same time upholding a high standard of fundamental-rights protection. Each side, and each Member State, can of course argue for placing more or less emphasis on a particular aspect – more or fewer powers, more or fewer safeguards, etc. What is ultimately appropriate is not least a question for national constitutional law and for the – hitherto often not clearly delimited – guarantees offered by the CFR. In any case, the EU-level debate should strive for balance, because the enhanced public-private cooperation proposed here does indeed pose major legal challenges.

https://doi.org/10.30709/eucrim-2023-030

III. Key Challenges

Data protection and the lack of a clear legal basis

Attempts to implement mechanisms for enhanced public-private cooperation are frequently thwarted by the lack of a clear legal basis. In fact, the law of many countries so far does not set forth rules for *voluntary* co-operation between the competent authorities and the private sector when they work together to prevent, detect, or investigate crime. So far, the law is primarily, and in some countries even exclusively, concerned with *coercive* measures (such as subpoenas and the seizure of documents), especially when performed as part of criminal investigations. Yet a one-sided focus on traditional, coercive instruments does not provide sufficient protection for the rights of customers whose data may be processed by obliged entities on behalf or at the instigation of the authorities. Without a clear legal basis to regulate public-private cooperation, neither the powers of the authorities nor those of obliged entities are clear. More specifically, the law of many countries so far lacks guidance on the lawfulness of a transfer of information to obliged entities by authorities and the extent to which authorities may be allowed to ask obliged entities to process customer data beyond what is required under the latter's CDD obligations. Similarly, as regards the powers of obliged entities, legal frameworks frequently lack clarity as to the extent to which obliged entities may process data when they do so largely or exclusively at the initiative of or on behalf of the authorities. Though public-private partnerships frequently seem to rely on the idea that existing CDD powers under the AML/CFT regulatory framework provide a sufficient legal basis, it can be unclear whether these powers do indeed suffice. In fact, CDD under the AML/CFT regulatory framework was originally conceived exclusively as a tool for obliged entities, not as a tool for the authorities. The nature of obliged entities' processing of their customer data can change significantly, however, and thereby lose the hallmarks of CDD in the conventional sense, if authorities become more and more involved in this processing. In any case, when seeking an appropriate legal basis under the General Data Protection Regulation (GDPR) for the voluntary processing of personal data at the initiative of or on behalf of the authorities (as would be necessary to enable various forms of enhanced public-private cooperation on AML/CFT), obliged entities will find – barring a special legal basis for voluntary public-private cooperation – only very limited possibilities.

The potentially high degree of intrusiveness of public-private data processing

Over the last several years, the European Court of Justice has established demanding requirements concerning data collection and transfer from private entities to public authorities. Further legal limits result from the case-law of the European Court of Human Rights. It is still unclear exactly how these requirements apply to the relationship between obliged entities and public authorities when they collaborate in the processing of customer data, and exactly what substantive and procedural safeguards for public-private cooperation in AML/CFT are required by EU data protection law.

Existing case-law provides criteria, however, to identify a few types of cooperation that regularly require particular legal guardrails. Insofar as a public-private cooperation measure aims at monitoring the activities of specific individuals, this can effectively amount to targeted, covert surveillance conducted by the authorities through the obliged entities. Depending on the nature and scope of the information sought, strong safeguards may be required, for example if the monitoring process in question provides insights into core areas of individuals' private life or if it enables the real-time geo-localisation of individuals. Similar considerations may apply if authorities ask obliged entities to conduct an in-depth analysis of an individual's past financial activities, especially if the authorities thereby try to obtain in-depth information about the targeted individual's private life. Lastly, case-law indicates the need for special safeguards if public-private cooperation aims at searching for individuals of interest by automatically and continuously screening vast numbers of unsuspicious customers and their transactions on behalf of the authorities.

https://doi.org/10.30709/eucrim-2023-030

De-risking and stigmatisation

The practice of de-risking and of adopting other measures to the detriment of customers (such as raising fees in response to a perceived higher risk) is already considered a major challenge for the AML/CFT framework. The problem is aggravated, however, by public-to-private information sharing. Up to now, de-risking was merely a problem arising in the (contractual) relationship between obliged entities and their customers. Yet when obliged entities' CDD is increasingly based (in part) on information that the authorities provide to the obliged entities, de-risking and other measures detrimental to customers will often be effectively attributable to the authorities and thereby impact the legality of the authorities' interaction with the obliged entities. As a consequence, public-to-private information sharing will need to be combined with stronger legal scrutiny of resultant adverse measures adopted by the obliged entity to the detriment of a customer.

At the same time, legislators' ability to effectively regulate obliged entities' risk management necessarily remains limited. After all, obliged entities necessarily enjoy contractual freedom. This means that the law may be unable to fully control the risks that public-to-private information sharing is bound to create for customers. This shortcoming constitutes a significant factor militating in favour of a cautious approach to public-to-private sharing, especially if the authorities share with obliged entities information that targets customers about whom only a suspicion – and not yet proof – of involvement in criminal activity exists. The more that such information may cause harm to the reputation of a customer, the more urgent the need for obliged entities to ensure that the information is not used for purposes other than those narrowly defined.

IV. Recommendations

The Recommendations are the result of a three-step analysis: understanding and categorising the various ways in which authorities and financial institutions are cooperating in the fight against money laundering and terrorism financing; subsequently identifying the relevant legal parameters under EU law; lastly, developing a legal framework for each of these different categories.

As for the need to categorise the various forms of public-private cooperation: Currently public-private cooperation is usually discussed using very vague and unspecific terminology – "partnership" being the most prominent example of such wording. To develop a legal framework, one needs to be more specific. Therefore, agreeing on a common terminology for different forms of cooperation is a key precondition for developing legislative Recommendations.

To this end, ParTFin analysed various forms of cooperation observed in existing partnerships, identified the various purposes pursued, and pinpointed the various methods of information sharing applied by the cooperating stakeholders. Five different categories of cooperation were able to be identified, three of them having the aim of supporting the crime-detection abilities of obliged entities, and two of them having the aim of supporting authorities. Oftentimes there is overlap between them, but it is still crucial to keep these separate categories in mind.

The five categories of cooperation revealed by ParTFin are:

- Threat warnings
- Risk notifications
- Risk indicators
- Financial analysis requests

https://doi.org/10.30709/eucrim-2023-030

- Financial monitoring requests

As for the development of a legal framework for each of these five categories, it was necessary to design them from scratch, because national legal orders have so far hardly addressed proactive public-private cooperation for AML/CFT purposes. As a consequence, the Recommendations will sound unfamiliar to many observers, not least to many lawyers. Discussing them requires patience and, above all, an understanding that the current state of affairs in AML/CFT cannot be considered satisfactory – neither from a law-enforcement nor from a fundamental-rights perspective.

1. Threat warnings

Meaning and purpose

By means of a threat warning, an investigative authority or another competent authority informs an obliged entity (or several obliged entities) about a specific criminal threat and names the specific individual or entity from whom the threat originates. A threat warning may, for example, serve to inform an obliged entity that specific individuals, who may be concealed behind shell companies, are linked to a criminal organisation and may currently be trying to abuse the entity. The warning is meant to enable the obliged entity to protect itself from the threat. If the individual or entity responsible for the threat is already known to the obliged entity, it will usually suffice to terminate the relevant relationship. If the obliged entity is not yet, at least not knowingly, in a relationship with the individual or entity in question, it can include the name of this individual or entity in the screening of customers and transactions, and thereby try to avoid exposure to the threat.

The purpose of threat warnings is to operationalise relevant information in the possession of authorities in order to protect obliged entities from criminal abuse. This corresponds to the observation that law enforcement authorities frequently come by information which, if shared with an obliged entity, would enable that entity to disrupt hidden financial crime plots. Often, however, such information is not brought to the attention of obliged entities, and it may sometimes not even be used for preventive purposes by the authorities themselves. In fact, authorities will in many cases be aware of an ongoing threat but nevertheless unable or unwilling, for various legal and practical reasons, to take direct action against the individual or entity at the origin of the threat. The resulting gap facilitates crime that could have been easily disrupted.

Field of application

Threat warnings could be issued by the police and judicial authorities during a criminal investigation. Warnings could, in particular, serve as a gateway for investigative authorities to provide feedback to an obliged entity following the filing of a SAR. However, threat warnings should not be limited to cases in which a SAR became relevant for an investigation; instead, legislators could consider introducing warnings as a standard measure available to investigative authorities.

In contrast, warnings should not be issued by FIUs, as FIUs will normally lack the complete picture of an investigation needed to be able to assess the threat potential of a particular criminal endeavour. In addition, powers to issue warnings should be provided when investigative authorities or administrative authorities (such as government ministries) learn about a threat outside a criminal investigation, for example based on information they received from non-EU authorities.

Concerns

The primary concern regarding threat warnings is that they can be erroneous. Given the prognostic nature of the assessment, there will often be no absolute certainty about whether a threat is actually present or not.

https://doi.org/10.30709/eucrim-2023-030

Available information is always backward-looking, but anticipating a threat typically means looking into the future. Naturally, issuing authorities can fall victim to miscalculation, for instance overestimating the danger posed by a particular individual. In addition, there can be cases where the available information subsequently turns out to be unreliable or incomplete. Given this uncertainty, it is important to note that threat warnings can heavily affect fundamental rights. Targeted individuals and entities may have their accounts closed and may be excluded from financial services and possibly even from entire markets due to an unsubstantiated suspicion.

Secondly, threat warnings can be problematic because obliged entities could use them in ways that do not correspond to their actual purpose, or could use them in an excessive manner. Out of a desire to avoid potential risks, an obliged entity might, for example, discontinue business relationships with individuals who share some characteristics with a person mentioned in a warning (for example individuals with similar spending habits or similar business activities), even if there is no reason to suspect that these individuals are involved in crime. How a warning is used by the obliged entity and whether the latter complies with any conditions set by the authorities can be difficult to verify.

As a third major vulnerability of threat warnings, the sharing of operational information with private entities can lead to a tipping-off of suspects and endanger investigations. Sensitive information can fall into the wrong hands, enabling criminals to cover up their tracks or providing them with new opportunities for crime. The unauthorised dissemination of warnings can also cause undue prejudice to the individuals and companies mentioned in those warnings, exposing them to widespread and lasting stigmatisation that may turn out to be unfounded or disproportionate.

Safeguards

Threat warnings label targeted individuals and entities as constituting an unacceptable financial crime risk, and thus essentially ask the addressed obliged entities to exclude these targets from financial services. It follows that the warnings can be highly intrusive, and that they therefore require the creation of a legal framework that includes adequate defence rights and ensures that the issuing of warnings is subject to effective judicial oversight. In light of this, threat warnings are usually unsuitable as part of a purely voluntary cooperation mechanism.

In order to address the danger of an erroneous prognosis, the issuing of threat warnings requires reliable evidence indicating that criminal abuse of a particular obliged entity, or multiple obliged entities, by a particular individual or entity is likely. In other words, the available information must give rise to a high probability that the individual or entity in question is already abusing, or will abuse, the obliged entity or obliged entities for the commission of financial crime. The target must be notified of the warning as soon as this is possible without endangering relevant investigations. Exceptions to this notification requirement may apply, in particular, to individuals and entities outside the EU – namely, insofar as they are not listed as beneficial owners in Member States' central bank-account registers or central beneficial-ownership registers and thus seemingly do not hold significant economic interests in the EU. In any case, after learning of the threat warning, targeted individuals and entities must be able to challenge the warning and the underlying threat assessment in court.

To prevent excessive implementation of warnings, obliged entities should be clearly instructed by the authorities on how to handle warnings. Most importantly, obliged entities may adopt adverse measures to the detriment of a customer on the basis of a warning only if there are reasonable grounds to suspect that this customer is related to the threat in question. To avoid circumvention of this rule, the content of a warning may be disclosed only to a small number of compliance staff members inside the obliged entity, and this content may generally not be included in the data used by the obliged entity for its regular CDD

https://doi.org/10.30709/eucrim-2023-030

screening. Individuals and entities affected by a warning must be able to effectively challenge its implementation through a complaint to the authority in charge of supervising obliged entities' data processing.

To avoid endangering investigations and prevent the undue stigmatisation of targeted persons, laws should require the addressees of a warning to treat it confidentially and not to disclose it to third parties, in some cases not even to other branches of the same obliged entity. Apparent breaches of such dissemination rules should be thoroughly investigated and be made subject to adequate sanctions. In any case, the scope of dissemination of a warning must be proportionate to the gravity of the particular threat in question. Consequently, the dissemination of a warning to a large number of obliged entities will be justified only under exceptional circumstances, whereas warnings addressed to only one obliged entity, or to only a small number of obliged entities, may be subject to less demanding conditions.

2. Risk Notifications

Meaning and purpose

Risk notifications allow the FIU (or potentially, in some cases, other authorities) to inform an obliged entity that a specific situation entails a high financial crime risk and should therefore be subject to additional CDD measures. This does not necessarily mean that the authorities have concrete information linking a customer to criminal activity. As is characteristic for a risk-based approach, a high risk may also result from particular features of a business relationship or transaction that signal merely a high statistical likelihood of criminal activity (for example when an individual opens numerous bank accounts within a short period of time without any apparent lawful reason). Risk notifications may single out specific customers or transactions; alternatively, they can point to other individual red flags (such as specific IP addresses or postal addresses) that the authorities believe to indicate a high financial crime risk.

Consequently, risk notifications – whether they refer to a specific customer or not – are meant to support obliged entities in their risk management by identifying situations in which they should scrutinise particular customers. This reflects the idea that the authorities are sometimes better placed than obliged entities to identify financial risks, even though it may still be speculative whether these dealings are actually linked to crime. Risk notifications thus allow obliged entities to put the spotlight on the applicable customers and, by performing additional CDD measures, check whether the filing of a SAR is called for. In other words, a risk notification requires the obliged entity to find out whether there are reasons to think that a high-risk situation is in fact related to crime.

Field of application

Risk notifications are a tool for FIUs to support obliged entities' implementation of the AML/CFT regulatory framework. As such, notifications may, in particular, be issued as a form of post-SAR feedback to the reporting entity. However, the FIU should be entitled to issue a notification even in the absence of a prior SAR. FIUs should usually exercise discretion as to whether or not to issue a notification in a particular case. However, legislators should consider defining situations in which an obliged entity may be entitled to receive a risk notification. This could be useful, especially if an obliged entity has repeatedly filed SARs regarding one and the same customer relationship over a long period of time without receiving any substantive feedback from the FIU or from investigative authorities. Insofar as the FIU enjoys discretion, the law should establish clear criteria for its case selection in order to avoid undue preferential treatment of some obliged entities.

https://doi.org/10.30709/eucrim-2023-030

Concerns

It is important to stress that risk notifications are meant merely to support obliged entities' CDD by identifying customers and transactions that should be subject to particular scrutiny. Conversely, risk notifications are not meant to say that specific customers are actually linked to crime. Herein lies the biggest challenge: when the authorities label a customer as constituting a high financial crime risk, it is very likely that obliged entities that receive this information will not subject this customer to additional scrutiny but will instead abstain from the relationship. In other words, instead of managing the risk, many obliged entities will prefer to avoid it altogether. However, this would mean that risk notifications fail their purpose. More importantly, affected customers would be exposed to de-risking and possibly lose vital business opportunities – in both cases essentially due to the authorities' interference, and without there necessarily being any evidence that these customers are involved in crime.

Yet risk notifications can negatively impact on affected customers even when obliged entities initially comply with the purpose of the notification and manage the risk instead of terminating their relationship with the affected customers. The fact that a customer was singled out as a high risk by the authorities is likely to harm this customer's reputation in the eyes of any obliged entity that learns about the notification, even if no concrete facts are found that link the customer to criminal activity. Obliged entities might assume, possibly rightly so, that dealings with such a customer may attract greater scrutiny from supervisory authorities and therefore entail a particular risk of being sanctioned for inadequate CDD.

Safeguards

To prevent risk notification from becoming a trigger for de-risking and similar consequences (such as the imposition of additional fees), the law must provide stringent rules on how obliged entities treat customers affected by a risk notification. As a minimum, an obliged entity should generally be under an obligation not to adopt adverse measures against such a customer during a waiting period. During this period, the obliged entity may take such measures only if it becomes aware of substantial reasons to file a SAR or if there are commercial reasons that require fundamental reassessment of the business relationship in question. To ensure adherence to this obligation, the obliged entity should inform the FIU about any significant changes in the business relationship during the waiting period.

As a crucial safeguard for protecting the reputation of a customer that has been subject to a notification, the recipient obliged entity should be strictly prohibited from sharing the notification and its content with third parties without prior authorisation by the FIU. This prohibition could be supplemented by additional safeguards, such as disclosing the risk notification to only a small number of vetted contact persons in the obliged entity or establishing a secure location where representatives from obliged entities interact with the authorities without having the possibility to produce records of the shared information. The law could empower the recipient obliged entity to require clarification from the FIU on whether its risk management of the customer in question is adequate. The obliged entity should, in this case, be entitled to rely on the FIU's assessment unless major changes subsequently occur in the risk profile of the customer in question.

Lastly, individuals and entities that were subject to a risk notification should be informed of the notification once this is no longer likely to tip off suspects or otherwise endanger investigations. They should furthermore be provided with effective remedies against an arbitrary issuing of risk notifications as well as against an unlawful handling of risk notifications by an obliged entity. Building on already-existing remedies required by the GDPR, such remedies should include the possibility to complain to the authority in charge of supervising the data processing of obliged entities. To ensure the effectiveness of such remedies, risk notifications and all communications between the FIU and obliged entities related to such notifications should be fully documented and accessible to this authority.

https://doi.org/10.30709/eucrim-2023-030

3. Risk Indicators

Risk indicators, whether in the form of typology papers or in any other form, are an established tool used, not least by FIUs and supervisory authorities, to provide the private sector with strategic information. Risk indicators do not point to particular business relationships or particular transactions, and therefore they typically do not constitute a significant interference with fundamental rights. As such, the issuing of risk indicators does not normally require extensive legal safeguards.

However, more recent practices show that risk indicators can go beyond the description of financial crime methods and additionally contain information about the national or geographic origin or other personal characteristics of perpetrators. The inclusion of such details may sometimes be desirable, for example when it enables risk indicators to highlight the activities of particular criminal organisations.

Legislators should provide appropriate safeguards for cases in which risk indicators have the potential to effectively single out customers with specific personal traits (for instance persons with a particular ethnic or religious background). For example, the issuing authority should be required in such cases to consult with an independent body to determine whether the potentially discriminatory effect of the envisioned risk indicator is justified by its added operational value in the fight against financial crime. Such safeguards would not only limit unintended consequences but, by providing legal certainty, also encourage competent authorities to improve the quality of risk indicators.

4. Financial Analysis Requests

Meaning and purpose

Via a financial analysis request, a competent authority asks an obliged entity to analyse its customer data in order to produce findings that may be of relevance for the authorities. Such requests can, for example, seek to determine whether a particular individual indirectly controls a particular company, or help retrace the flow of money through a long chain of seemingly unconnected companies. For the requested analysis to produce meaningful findings, the requesting authority will regularly need to provide the obliged entity with information about suspects or with other tactical or strategic information. The more relevant the information shared with the obliged entity, the more the obliged entity will usually be able to direct its analysis in ways that produce added value for the authorities.

Financial analysis requests essentially reflect the idea that it may be more useful for the authorities if obliged entities analyse their data themselves instead of transferring bulk data to the authorities. Often, such a transfer of bulk data will be unfeasible in any case. Authorities will sometimes also lack the technical infrastructure to perform high-quality analyses. Moreover, unlike the authorities, obliged entities will frequently be able to directly access information held by branches and subsidiaries in other countries.

Field of application

Financial analysis requests should be available primarily to investigative authorities in the context of criminal investigations and related administrative proceedings, not least in proceedings aimed at non-conviction-based confiscation. Although some Member States may already accept financial analysis requests as part of the conventional powers under the law of criminal procedure (notably powers to subpoena obliged entities), there is to date certainly no consensus on whether the existing powers of competent authorities cover such requests to gather evidence or at least intelligence. Beyond making financial analysis requests available to investigative authorities in the contexts described above, legislators could consider making financial analysis requests available to FIUs in support of their operational analyses.

https://doi.org/10.30709/eucrim-2023-030

Concerns

Financial analysis requests raise problems, first of all, because they can entail highly intrusive processing of personal data. Analysing transaction data and other data collected for the purpose of CDD can yield in-depth insights into a person's private life. The intrusiveness of the analysis is further intensified if the obliged entity, in its analysis, includes information about a person's online activities, such as her use of social networks.

Furthermore, financial analysis requests can be problematic as regards the reliability of the resulting findings. Oftentimes the conclusions of an analysis will, to a greater or lesser extent, be based on unverified assumptions, for example assumptions about the beneficial owner of a company, even though these assumptions will not necessarily be apparent from the analysis result that the obliged entity provides to the requesting authority. The result of a financial analysis can give rise to doubts about its completeness, bearing in mind possible conflicts of interest in cases in which the activities of a suspected customer might at the same time involve compliance failings on the part of the obliged entity.

Financial analysis requests can also raise concerns insofar as the disclosure of sensitive information to obliged entities might produce unintended detrimental consequences, in particular de-risking, for affected customers. Stigmatising detrimental consequences can arise with regard to any affected customer, which is especially concerning because affected customers may include individuals and companies against whom the criminal suspicion is only weak so far, and, in some cases, customers who are not even suspects.

Safeguards

To address data protection concerns, the requesting authority should specify how the obliged entity must analyse its data, in particular by defining and limiting the scope and nature of customer data to be included in the analysis. Sensitive insights into a person's private life should be sought only when this is proportionate to the seriousness of the criminality at stake and to the degree of suspicion in the particular case. In order to uncover possible sources of error, including a potential discriminatory bias, in the results of an analysis that has been conducted in response to an analysis request, the requesting authority may be required to gain an understanding of the data-processing methods used for the analysis by the obliged entity. If a financial analysis is meant to target individuals, prior authorisation by a judicial or other independent body, or oversight by such a body of the issuing and implementation of the analysis request, can constitute an important safeguard.

As regards the reliability concerns associated with financial analysis requests, legislation could provide guidance on the subsequent use of any resulting findings. Insofar as the analysis is largely automated and the underlying facts are not fully transparent, the findings of analyses conducted in response to requests should generally be used only as investigative leads, not as evidence. Furthermore, legislation should ensure that obliged entities are under an obligation not to withhold any relevant information from the requesting authority when responding to a financial analysis request.

Crucially, to reduce the probability of unintended consequences, obliged entities that receive a financial analysis request should be strictly prohibited from sharing the request and its content with third parties without prior authorisation. To prevent financial analysis requests from prompting de-risking, investigative authorities could be empowered to inform recipient obliged entities whether the individuals or companies targeted by the requests they have received constitute an enhanced financial crime risk. If a recipient obliged entity is informed in this way that a particular targeted customer does not constitute such a risk, and if there are no other significant reasons to the contrary, the obliged entity should be entitled not to treat this customer as a financial crime risk, and should be entitled to rely on this approach vis-à-vis the supervisory authority if this authority criticises the adequacy of the obliged entity's CDD with regard to this customer.

https://doi.org/10.30709/eucrim-2023-030

If a financial analysis request is issued by an FIU or other authority before a criminal investigation against the targeted person has been opened, additional safeguards should apply in order to protect as-yet unsuspected individuals. In such cases, the above-described safeguards for risk notifications should apply, because the request will, as regards the recipient obliged entity's risk assessment, usually have the effect of implicitly labelling the targeted customer as an enhanced financial crime risk.

5. Financial Monitoring Requests

Financial *monitoring* requests go beyond financial *analysis* requests in that they ask obliged entities not only to analyse customer data but also to collect additional data for the benefit of authorities. Monitoring requests can take various forms, from a request to monitor the activities in a particular payment account to a request to gather extensive information about the activities of a particular customer or in an entire business segment. While the relevant problems and respective solutions largely correspond to those described above for financial analysis requests, some additional challenges need to be addressed. In particular, as monitoring requests can amount to covert surveillance, they will need to respect particularly demanding legal standards, such as prior authorisation by a judicial or other independent body, and subsequent notification of targeted individuals if such notification no longer endangers the investigation.

1. Security Council resolution 2462 (2019), para. 22.↩
2. FATF, *Guidance on Private Sector Information Sharing* (Paris, 2017), p. 27, available at: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html> accessed 13 February 2024.↩
3. European Commission, Commission Staff Working Document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing of 27 October 2022, SWD(2022) 347 final.↩
4. N. J. Maxwell, Future of Financial Intelligence Sharing (FFIS) – Survey Report "Five years of growth in public–private financial information-sharing partnerships to tackle crime," August 2020, available at: <https://www.gcffc.org/wp-content/uploads/2020/08/FFIS-Report-Five-Years-of-Growth-of-Public-Private-Partnerships-to-Fight-Financial-Crime-18-Aug-2020.pdf> accessed 13 February 2024.↩
5. European Data Protection Board letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations of 28 March 2023, OUT2023-0015, available at: <https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf> accessed 13 February 2024.↩

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union