Non-paper on enhancing gatekeepers' effectiveness through cooperation and innovation

Denmark, Germany and the Netherlands (hereafter: the signatories) strongly encourage that Member States seize the opportunity to ensure that the new European framework for anti-money laundering and combatting the financing of terrorism (hereafter: AML/CFT) is fit for the future. The new framework should enhance gatekeepers' effectiveness through cooperation[1] and innovation and at the same time place adequate safeguards to ensure correct performance of the tasks and data protection in accordance with the General Data Protection Regulation (hereafter: GDPR).

The key element of the global and European AML/CFT framework is that obliged entities, as gatekeepers of the financial system, identify risks and take measures accordingly. Despite increasing efforts and allocation of resources by obliged entities to AML/CFT, the effectiveness of the approach to fight money laundering and terrorist financing (hereafter: ML/TF) can be improved. There is no single target, but there is room for improvement regarding shorter detection times[2], a reduction in the number of false alerts raised in existing transaction monitoring systems[3], and a higher success rate in detecting complex money laundering schemes. In order to allow obliged entities to improve their approach in these areas, we need to ensure that the AML/CFT framework allows obliged entities to rethink and innovate their AML/CFT efforts and increase cooperation.

The increasing complexity and sophistication of ML/TF methods particularly warrant innovation and enhanced cooperation to keep up with the developments. Cooperation and innovation are important and will become increasingly so in understanding, identifying and mitigating ML/TF threats.

Innovation and cooperation allow gatekeepers to acquire better in-depth insight in possible risks and to take action accordingly and at a faster pace. It can also support smaller obliged entities with fewer resources in obtaining efficient AML/CFT-tools. Sharing of data between gatekeepers is key to successful cooperation.

---

[1] 'Cooperation' in this non-paper refers to both public-private and private-private cooperation.

[2] In 2020, the Danish Central Bank facilitated a "Proof of Concept (POC)" in corporation with other Danish authorities (the Danish FIU, DFSA etc.) and a large Danish credit institution. Focus was on estimating potential gains from a more databased approach to transaction monitoring. Among other things, the results indicate that further use of data (including suspicious transactions reports) can increase detection times of suspicious transactions by up to ten weeks.

[3] In 2019, the Danish FSA did a comprehensive evaluation of transaction monitoring in a subset of large Danish credit institutions. Among other things, the evaluation showed that in the period from 1 October 2018 to 30 September 2019, an average of 4,450 risk flags per month were raised across the credit institutions surveyed, but only 5 per cent of these risk flags led to a report to the Danish FIU.

Fueled by new technological possibilities new initiatives have emerged in the signatories' states focusing on increasing effectiveness and quality of AML/CFT efforts. Examples are joint utilities focused on transaction monitoring, know your customer utilities, and other compliance solutions developed by the private sector (so-called RegTechs). These initiatives have different designs: some allow obliged entities to share information on transactions in order to acquire better insights in ML/TF risks and methods, others take the form of a specialized entity supporting obliged entities in the performance of their know your customer obligations.

- Examples of these initiatives are the Danish AML/TEK and FALK project[4] and the Dutch TMNL. In AML/TEK obliged entities are projected to share information on ML/TF risks identified with certain customers during CDD to prevent off boarded customers simply switching between obliged entities to regain access to the financial system and continue their activities.
- Within FALK and TMNL banks are projected to pool transactions to identify high risk transaction chains that would otherwise go undetected by individual banks.

The preliminary results from these initiatives indicate that sharing of data and/or outsourcing tasks can contribute to performing obliged entities' roles, and that this can be achieved with the necessary safeguards in terms of data protection, especially with regard to the principles of necessity and proportionality, without compromising the ultimate responsibility of obliged entities to comply with AML/CFT regulations individually.

These initiatives have thereby demonstrated a gap in the current AML/CFT framework. To fully realize the potential of such initiatives, the AML/CFT framework should provide clear rules on data sharing, responsibilities and adequate safeguards. These initiatives build on sharing relevant customer and transaction data from multiple obliged entities within entities established to perform specialized tasks. Information sharing and outsourcing are driving factors for innovation in AML/CFT. The new AML/CFT framework should accommodate such initiatives by allowing for sufficient room for innovation and cooperation, while imposing adequate safeguards.

The current AMLR proposal does not sufficiently provide the necessary clarity or scope on data sharing and cooperation, while maintaining some and introducing additional impediments. These impediments are:

- The restriction of the outsourcing tasks (article 40);
- The absence of clarity under which circumstances obliged entities are allowed to share data with each other (article 55); and

[4] The FALK project is currently set on hold due to the restrictive nature of the prohibition of disclosure. The full value proposition requires that participating obliged entities can share suspicious transaction reports on customers involved in identified criminal networks.

- The very restrictive prohibition of disclosure (article 54).

The signatories propose to amend these articles to allow obliged entities to strengthen their gatekeepers' role through cooperation and innovation, with adequate safeguards and a clear constitution of the responsibility of the obliged entities.

Article 40 – outsourcing

The signatories explicitly affirm the principle that obliged entities are ultimately individually responsible for compliance with the AML/CFT framework and that they should have sufficient control and understanding of their obligations. This applies regardless whether certain tasks are outsourced. However, the signatories deem the currently proposed restrictions on outsourcing disproportionate and ineffective. Outsourcing could provide obliged entities, especially smaller ones, with means to utilise the expertise and effectiveness of specialized entities, thereby increasing their effectiveness of AML/CFT compliance, while improving their efficiency. Therefore, instead of prohibiting outsourcing of tasks, the signatories propose to enshrine safeguards on outsourcing within the scope of internal controls of obliged entities.

Article 40
Outsourcing

1. Obliged entities may outsource tasks deriving from requirements under this Regulation ~~for the purpose of performing customer due diligence~~ to an agent or external service provider, whether a natural or legal person, with the exception of natural or legal persons residing or established in third countries identified pursuant to Section 2 of this Chapter. The obliged entity notifies the supervisory authority about the outsourcing before the agent or external service provider starts the activities for the obliged entity.
The obliged entity ~~shall~~ remains fully liable for any action connected to the outsourced activities of agents or external service providers to which activities are outsourced and remains responsible as controller pursuant article 4 (7) of Regulation (EU) 2016/679 for any personal data processed for the purpose of the outsourced tasks.
2. The tasks outsourced pursuant to paragraph 1 shall not be undertaken in such way as to impair materially the quality of the obliged entity's measures and procedures to comply with the requirements of this Regulation and of Regulation *[please insert reference – proposal for a recast of Regulation (EU) 2015/847 - COM/2021/422 final]*. The following tasks shall not be outsourced under any circumstances:
(a) the approval of the obliged entity's risk assessment according to Article 8 and of its policies, controls and procedures according to Article 7 of this Regulation;
(b) the responsibility to be in compliance with this Regulation.
~~(b) the internal controls in place pursuant to Article 7 ;~~
~~(c) the drawing up and approval of the obliged entity's policies, controls and procedures to comply with the requirements of this Regulation;~~
~~(d) the attribution of a risk profile to a prospective client and the entering into a business relationship with that client;~~
~~(e) the identification of criteria for the detection of suspicious or unusual transactions and activities;~~
~~(f) the reporting of suspicious activities or threshold based declarations to the FIU pursuant to Article 50.~~
Any subsequent outsourcing of tasks by the agent or external service provider to other agents or external service providers is not allowed.
3. Before ~~Where~~ an obliged entity outsources a task pursuant to paragraph 1, it shall ascertain itself that the agent or external service provider is reliable and sufficiently qualified to fulfill its obligations. Furthermore, it has to ensure that the agent or external service provider applies the measures and procedures adopted by the obliged entity. The conditions for the performance of such tasks shall be laid down in a written agreement between the obliged entity and the agent or the external service provider ~~outsourced entity~~. The obliged entity shall perform regular controls to ascertain the effective implementation of such measures and procedures by the outsourced

entity. The frequency of such controls shall be determined on the basis of the critical nature of the tasks outsourced.
4. Obliged entities shall ensure that outsourcing is not undertaken in such way as to impair materially the ability of the supervisory authorities to monitor and retrace the obliged entity's compliance with all of the requirements laid down in this Regulation.

In addition, in order to underline the importance of compliance with data protection rules, the following clarifying new recital 63a should be introduced:

(63a) When outsourcing tasks deriving from requirements under this Regulation, the obliged entity remains the controller under Regulation (EU) 2016/679 and thus would have to ensure full compliance with the requirements of Regulation (EU) 2016/679. Outsourcing tasks to agents or external service providers in third countries has to follow the requirements of Chapter V of Regulation (EU) 2016/679; processors from third countries would also have to designate in writing a representative in the Union (Article 27 of Regulation (EU) 2016/679). Furthermore, as this would regularly constitute processing within the meaning of Article 28 of Regulation (EU) 2016/679, a contract or other legal act would have to be concluded with the agent or external service provider. In that context, in order to ensure that the supervisory capacity of the data protection supervisory authorities is not restricted due to multiple outsourcing, agents or external service providers are not allowed to outsource the tasks mandated to them on their behalf.

Article 55 - processing of personal data

The current proposal recognizes the need for obliged entities to process personal data in order to fulfil the requirements following from the regulation. This is a necessary addition to the framework. The current proposal does not, however, provide clarity on how and when (or even if) obliged entities are allowed to exchange information with other obliged entities and which form the processing of data may take. Therefore, the signatories propose to offer more clarification regarding the possibilities and conditions for the sharing and processing of data.

Additionally, the signatories propose to clarify that Member States may allow (specific) obliged entities to set up joint utilities, where personal data can be shared for the purposes of the prevention of money laundering and terrorist financing. This would for example allow transactions to be pooled in order to identify high risk transaction chains that would otherwise go undetected by individual obliged entities. Since joint utilities can take on different forms, it is more suitable to leave it to national law to prescribe the specific measures and safeguards that are required for the specific joint utility. The signatories do propose that it is laid down on EU-level that these safeguards should at least include measures and safeguards ensuring that the obliged entity's participation in a joint utility does not compromise its compliance with this Regulation or the ability of supervisory authorities to monitor and retrace the obliged entity's compliance with the requirement of this Regulation. Furthermore, when sharing personal data in joint utilities, measures and safeguards should be put in place to ensure compliance with the GDPR.

Article 55

Processing of ~~certain categories of~~ personal data

1. To the extent that it is ~~strictly~~ necessary and proportionate for the purposes of preventing money laundering and terrorist financing, obliged entities may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and personal data relating to criminal convictions and offences referred to in Article 10 of that Regulation subject to the safeguards provided for in paragraphs 2 and 3.
2. Obliged entities shall be able to process personal data covered by Article 9 of Regulation (EU) 2016/679 provided that:
(a) obliged entities inform their customer or prospective customers that such categories of data may be processed for the purpose of complying with the requirements of this Regulation;
(b) the data originate from reliable sources, are accurate and up-to-date;
(c) the obliged entity adopts measures of a high level of security in accordance with Article 32 of Regulation (EU) 2016/679, in particular in terms of confidentiality.
3. In addition to paragraph 2, obliged entities shall be able to process personal data covered by Article 10 of Regulation (EU) 2016/679, in particular in terms of confidentiality.
4. Obliged entities may process p~~P~~ersonal data (Article 4 (1) of Regulation (EU) 2016/679) ~~shall be processed by obliged entities~~ on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing ~~and shall not be further processed in a way that is incompatible with those purposes~~.
5. Without prejudice to Article 54 and to the extent that is necessary and proportionate, obliged entities may share between each other personal data for the purposes of the prevention of money laundering and terrorist financing, provided that these matters involve abnormalities or unusual circumstances indicating money laundering or terrorist financing. Further processing of personal data under this paragraph for other, in particular commercial purposes, shall be prohibited.
6. Without prejudice to further obligations under Regulation (EU) 2016/679 and [EU-AI Regulation], the processing of personal data according to paragraph 4 may be conducted by means of automated decision-making, including profiling (Article 4 (3) of Regulation (EU) 2016/679), or artificial-intelligence systems as defined in [Article 3 of Regulation insert title EU-AI-Reg; COM(2021) 206 final)], provided that:
- the obliged entity has conducted the necessary data protection impact assessment according to Article 35 (3) (a) of Regulation (EU) 2016/679 prior to the processing;
- if the processing takes place in a third country, the requirements of Chapter V of Regulation (EU) 2016/679 are met;
- the processing of personal data only comprises data which an obliged entity has collected in the course of performing its customer due diligence obligations, including, in particular, the ongoing monitoring pursuant to Article 20.
7. By way of derogation from paragraph 5, each Member State may lay down in national law that obliged entities may share personal data for the purposes of the prevention of money laundering and terrorist financing within joint utilities. Those rules shall in particular include measures and safeguards to ensure compliance with this Regulation, Regulation (EU) 2016/679 and the ability of the supervisory authorities to monitor and retrace the obliged entity's compliance with the requirements laid down in this Regulation.

Article 2

Definitions

(37) 'Joint utility' means a formal cooperation, established by Member States' national law, between obliged entities with the purpose of supplementing compliance with the requirements set forth in this Regulation through cooperation and by sharing information.

Article 54 – Prohibition of disclosure

The provision on "tipping off" in The Financial Action Task Force (hereafter: FATF) Recommendation 21 is not intended to inhibit information sharing between obliged entities, but to ensure that potential criminals are not alerted to law enforcement authorities' efforts to investigate, prosecute and disrupt ML/TF activities. The current provision on disclosure poses a barrier to new initiatives that aim to increase effectiveness through increased cooperation and innovation. For example, it provides a direct barrier to assess risky networks identified in

initiatives such as the FALK project on a fully informed basis. Furthermore, it conflicts with the highly prioritized FATF agenda on better use of technology and data in the fight against ML/TF. The FATF has published preliminary views on the use of technology and data pooling.[5] The FATF's ongoing work focuses on materializing these views, for example by focusing on identifying the necessary safeguards to allow for further information sharing without compromising data protection requirements.

The future AML/CFT framework should not hinder the important efforts in this area. At the same time, necessary safeguards for privacy, data protection and ultimate responsibilities are conditional for an increase in cooperation and innovation. The key principles in such safeguards should be governance, supervision and harmonization of requirements for cooperation and information sharing. Therefore, the signatories propose to allow for disclosure between obliged entities within joint utilities. Since Member States are required to introduce various safeguards pursuant to article 55 (7), the "tipping off" risk can be mitigated, while the risk of introducing new issues with "de-risking" and "blacklisting" can be minimized.

Additionally, the signatories propose to broaden the possibility for disclosure. The current condition for disclosure – 'same customer, same transaction' – provides a barrier for two obliged entities to inform each other about potential risks associated with a specific transaction between two customers. Removing this barrier can facilitate more informed assessments, support higher quality suspicious transaction reports and support cooperation in the detection of ML/TF. Therefore, the signatories propose to enable disclosure in cases relating to the same transaction.

Article 54 **Prohibition of disclosure**
1. Obliged entities and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in accordance with Article 50 or 51 or that a money laundering or terrorist financing analysis is being, or may be, carried out.
2. Paragraph 1 shall not apply to disclosures to competent authorities and to self-regulatory bodies where they perform supervisory functions, or to disclosure for the purposes of investigating and prosecuting money laundering, terrorist financing and other criminal activity.
3. By way of derogation from paragraph 1, disclosure may take place between the obliged entities that belong to the same group, or between those entities and their branches and subsidiaries established in third countries, provided that those branches and subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 13, and that the group-wide policies and procedures comply with the requirements set out in this Regulation.
3a. By way of derogation from paragraph 1, disclosure may take place between obliged entities within joint utilities.
4. By way of derogation from paragraph 1, disclosure may take place between the obliged entities as referred to in Article 3, points (3)(a) and (b), or entities from third countries which impose requirements equivalent to those laid down in this Regulation, who perform their professional activities, whether as employees or not, within the

[5] https://www.fatf-gafi.org/publications/digitaltransformation/digital-transformation.html?hf=10&b=0&s=desc(fatf_releasedate).

same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control, including networks or partnerships.

5. For obliged entities referred to in Article 3, points (1), (2), (3)(a) and (b), in cases relating to ~~the same customer and~~ the same transaction involving two or more obliged entities, and by way of derogation from paragraph 1, disclosure may take place between the relevant obliged entities provided that they are located in the Union, or with entities in a third country which imposes requirements equivalent to those laid down in this Regulation, and that they ~~are from the same category of obliged entities~~ are subject to professional secrecy and personal data protection requirements.

5a. By way of derogation from paragraph 1, disclosure may take place between an obliged entity and its agent or service provider to which it has outsourced activities related to customer identification and due diligence measures according to Chapter III of this Regulation or reporting as referred to in Articles 50 and 51 of this Regulation.

6. Where the obliged entities referred to in Article 3, point (3)(a) and (b), seek to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1.

7. By [2 years from the entry into force of this Regulation], AMLA shall develop draft regulatory technical standards and submit them to the Commission for adoption. Those draft regulatory technical standards shall specify the minimum standards for sharing of information between obliged entities subject to the exemptions in paragraph 3a, 4 and 5 in this Article.