

AML: key success factors to boost EU effectiveness

1. It will take three years to implement the single directly applicable legal basis for anti money laundering (AML) and establish Anti Money Laundering Authority (AMLA)

The Chair explained that the aim of the European Commission's 2022 AML package was to create a new basis for Europe's AML regime. The package standardises the legal requirements for obliged entities, which are mainly in the private sector. In the future, there will be a single directly applicable legal basis in the form of a regulation. This will be supplemented by the establishment of AMLA, which will be a European standard setter, a supervisor, and a platform for information exchange between financial intelligence units (FIUs).

In the financial sector, AMLA will directly supervise high risk companies, instruct AML colleges, and even have the power to assume national supervision. In the non financial sector, AMLA will primarily conduct oversight via peer reviews. The trilogue negotiations on the AML package were successfully concluded in January 2024. In view of the upcoming Parliament elections, any delay could have caused considerable damage to the fight against money laundering.

There will be a transition period of three years for the regulation to be applied and the directive to be implemented. Until that point, AMLA must be established and strengthened. The level 2 and level 3 texts must be developed to ensure that the provisions are sufficiently detailed to be directly applicable in practice. One of the key challenges will be to bring together AML and data protection. This is another success in the substantive law. There will now be a clear legal basis for information exchange, which creates certainty for the private sector.

2. Key success factors for creating an effective AMLA: cross-border cooperation, including data analysis; matching supervision with risk; human and technical resources; and ever increasing agility

A regulator commented that there is an opportunity for AMLA to learn from the establishment of the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA).

There are four key factors that will ensure AMLA is successful. The first is international cooperation and convergence. Effective AML is only possible through cross border cooperation. The European supervisory authorities (ESAs) have considerable experience of international supervisory cooperation, from which AMLA can learn. Secondly, AMLA must practise high quality risk based supervision. Currently, the data required to undertake risk based supervision is not collected effectively. Consolidating the data sent to the ESAs will eliminate redundancy and duplication, reducing the burden on the financial sector. Thirdly, AMLA's procedures will need both resources and interconnectivity. The final key factor is education. AML is evolving constantly as entities find new ways to avoid the rules. AMLA must try to continuously learn and adapt to these challenges. It must be able to develop new tools quickly in response to new threats.

The Chair observed that the AML legal text shows that the legislators have already learned some lessons from the establishment of the other ESAs.

3. National authorities are preparing for the new AML framework and AMLA

3.1 Under the umbrella of the EBA, national authorities are adapting their processes, systems, governance arrangements, staff and cultures

A regulator explained that the preparation for AMLA is already underway. Initially, AMLA will have a large amount of work to do with few staff. At national level, preparatory work is being done by national supervisory authorities and FIUs. Many national authorities, including the Austrian Financial Market Authority (FMA), have set up project like structures to manage the transition to AMLA. This is a critical process. All national authorities need to study their processes, systems, governance arrangements, staff, and culture. At European level, there is a need for coordination and collaboration. The efforts to prepare supervisors and FIUs will be a critical factor in the success of AMLA. The EBA has created a forum to allow European supervisors to discuss the practical implications of AMLA. This forum has determined some common priorities to ensure that the preparatory work is efficient and coordinated. The new model will be about common risk based supervision. The analysis of risk will play an important role in determining which institutions fall under AMLA's direct supervision. Supervisors will have to decide how to collaborate in terms of data management and the exchange of information. Ultimately, AMLA will only be as good as the national supervisors joining forces under the new supervisory model.

A regulator emphasised that cooperation between national competent authorities (NCAs) will be the most crucial success factor. In the past few months, Malta's Financial Intelligence Analysis Unit (FIAU) and the Malta Financial Services Authority (MFSA) have created independent structures to assess AMLA's impact on processes such as licensing, risk assessments, supervision, and enforcement. As commented above, AMLA's effectiveness is also dependent on the procedural and operational maturity of the EU Member State's competent authorities on AML/CFT. From what is already observable at present, it will be necessary for some NCAs to gather more data/information which they are not currently gathering from both their respective industries and other supervisory authorities. Still, the developments required will not be limited to this, NCAs will need to assess their overall risk assessment, supervisory, and enforcement processes to facilitate European consistency. Preparatory work is currently being undertaken by both the European Banking Authority in collaboration with NCAs to facilitate Europe's transition to AMLA as a dedicated supervisor.

An industry representative highlighted the importance of having agile systems. Obligated entities will need to have easily modifiable systems for transaction monitoring, case management and Know Your Customer (KYC) and the ability to implement new requirements. It is not practical for an obliged entity to develop new systems and protocols in response to each new regulatory obligation.

3.2 After regulatory adaptation and clarification, which is the immediate priority for member states, there should be a period of regulatory stability

A regulator stated that regulatory adaptation is the most urgent priority. AMLA will have to deliver around 70 mandates in the next two years. It will be very difficult for AMLA to achieve this task if it is forced to rely on national supervisors. National supervisors will need to coordinate and deliver the preparatory work, which AMLA will pick up and transform into a single rulebook.

A regulator noted that both the Maltese FIAU as the single regulator for AML/CFT and the MFSA have started to engage with stakeholders and other European and local authorities facilitate the transition to AMLA. Particularly, the MFSA, as the Maltese financial services regulator, houses a dedicated committee intended to centralise the consideration of AML/CFT, including the very major changes that will be required because of the implementation of AMLA. At European level, the EBA, through its Standing Committee on AML/CFT (AMLSC), is conducting a significant amount of preparatory work alongside NCAs, such as by taking stock of risk assessment and supervisory practices across all the Member States. The AMLSC significantly facilitates the ESAs and NCAs discussions on the implementation of the AML package.

An industry speaker considered that there should be a period of institutional stability once the framework is implemented. Over the last 30 years, the EU's preventive AML regulatory framework has been frequently adjusted. Institutional stability will get the best out of the system. The main challenge for AMLA will be to complete the

single rulebook. A significant number of implementing technical standards (ITS) and regulatory technical standards (RTS) will have to be drafted in a very short timeframe. The challenge will be to communicate this to obliged entities in a clear and timely way to ensure they understand the rules are, how the rules should be interpreted, what the supervisory expectations are and what the supervisory cycle will be. Obligated entities can then prepare themselves ahead of the deadline. AMLA will try to instil a common supervisory culture by engaging with domestic AML authorities and learning from them. By supporting and assisting the domestic authorities AMLA will come to be regarded as a trustful and reliable partner.

An industry representative emphasised that the introduction of standardised rules across Europe is good news for banks. It is shocking how many countries in Europe have implemented directives in very different ways. Although these are new regulatory requirements, this consistency should be very helpful. The priority of banks is to comply with current regulatory requirements. The banks do not want to be caught off guard by the new requirements. They are trying to conclude their remediation programmes to ensure their 'house is clean'.

3.3 The use of the tools developed for the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM) could benefit AMLA and contribute to the global credibility of the EU AML model

An industry speaker noted that AMLA bears some similarities with the SSM and the SRM. Many of the tools developed at SSM level could enrich AMLA's toolbox. However, there are also sizable differences. First, AMLA's scope will be sectorally broader and geographically more fragmented. Secondly, the risk profiles allocated to obliged entities will be dissimilar to those in the prudential domain. The risk is not specifically proportional to size and is more complex to define. Thirdly, AMLA will need to ensure that FIUs work together, exchange information and investigate cross border cases. AMLA will need to use the full range of tools available, including a new version of FIU.net. FIUs should also provide feedback to obliged entities about the effectiveness of their transaction monitoring systems. AMLA will enhance the credibility of the EU model globally. For AMLA to be regarded as a trusted and influential partner in the definition of further standards and requirements at Financial Action Task Force (FATF) level, the European model will have to be regarded as a global point of reference.

An industry representative commented that banks will need to have access to data. When an institution comes under SSM supervision, the ECB asks for many different types of data. For AMLA to be successful, it will have to do the same. Banks and other entities want to be able to send supervisors the correct data immediately. Ultimately, the governance framework for any new regulatory requirement should be useful; it should not be a bureaucratic nightmare. The creation of a streamlined and effective governance framework will ensure that entities know what to do and who to work with.

4. For AMLA to be able to analyse bulk data effectively, it will require technology, trained individuals, Joint Investigation Teams (JITs), an outcome based approach and agility

A regulator stated that effective AML/CFT is dependent on collaboration, cooperation, and the exchange of information. For AML/CFT efforts to be effective, supervisors need to be able to collect and analyse bulk data. Given the difficulty of processing such a large volume of data, technology and IT systems will play a key role in achieving an effective AMLA, exacerbating the importance of utilising AI/Machine Learning technologies. Secondly, there is also a need for appropriately trained individuals who can intelligently analyse said data and. Thirdly, the key to identifying issues and taking action is the processing and analysis of data. NCAs will be able to help AMLA by using task forces and Joint Supervisory Teams (JITs), in which officers are able to access data and exchange and analyse information in bulk. Fourthly, AMLA will need to take an outcome based approach towards its supervision to facilitate its supervisory effectiveness as a new European agency. A great deal of time and effort will need to be invested in the creation of a risk based approach to supervision, intelligence sharing, decision-making and cooperation with law enforcement.

An industry representative highlighted the importance of focusing on how to fight financial crime legislatively. Banks are filing thousands of alerts with FIUs every day. Currently, the regulatory framework obliges banks to file alerts when they detect anything suspicious. A bank is not a law enforcement entity, however. It does not know whether someone is conducting a criminal activity or not. Consequently, banks are filing a very large quantity of useless alerts. The potential of being subjected to a detailed regulatory investigation induces the banks to file these so called defensive alerts. Fighting financial crime effectively means only filing relevant alerts with the FIU. Banks have spent billions of euros trying to build something effective, but the current system does not work.

An industry speaker agreed that effective transaction monitoring is one of the main challenges faced by obliged entities. There are limitations on transaction monitoring, such as limits to the capabilities of rule based transaction monitoring systems, the siloed approach in which obliged entities only see particular customer transactions and the lack of feedback from FIUs. These limitations can in part be overcome by using technology. AI and machine learning can be very useful tools for AML. These technologies can identify links between data points and identify patterns in transactions. These tools need (to process) massive amounts of data, however, which raises some data privacy concerns.

5. Balancing effective AML with privacy and data protection

The Chair commented that it is also very important to discuss balancing effective AML exchange with privacy

and data protection. It is very important to cooperate on this topic with colleagues who work in data protection.

5.1 Privacy and data protection are fundamental rights

A regulator explained that privacy and data protection are fundamental rights enshrined in articles 7 and 8 of the EU Charter of Fundamental Rights, but they are not absolute. They must be considered alongside other policy objectives and legitimate interests in EU law. Finding a balance can sometimes be complicated, but the Court of Justice of the European Union is clear that these fundamental rights prevail. The ruling on the register of beneficial ownership should serve as a reminder of the need to strike the right balance. The Chair observed that the uncertainty of the rules is a significant problem, but it is very positive to see that European legislators have tried to strike a balance and create a clear basis for the rules.

5.2 Network analysis and transaction monitoring

An industry representative stated that society recoups around 1% of the \$800 billion to \$2 trillion laundered globally every year. The current system does not work. It does not recover what should be recovered. For this reason, it is important to consider what works and what does not work. Network analysis and transaction monitoring is very important. These systems enable society to 'follow the money'. The goal of the regulatory requirements is to fight financial crime. There have been discussions about how the new regulatory requirements will classify the mayors of small towns in Europe as politically exposed persons (PEPs). This will have no added value in the fight against financial crime.

What does work is data sharing. Transaction Monitoring Netherlands (TMNL) is a data-sharing initiative. In July 2020, five Dutch banks agreed to share transaction data anonymously. Although the data is anonymised, many people are surprised to hear that this data is being shared. Their personal records are not shared, however. The key responsibility of a bank is to manage data. There is nothing new about banks having access to data. The question is how to share this data in an anonymised way to identify the bad actors trying to launder dirty money through the financial system.

TMNL is already anonymously sharing data on small businesses. The system works. Banks in TMNL have been filing alerts to the FIU that would not otherwise have been detected. These bad actors are professional money launderers working for criminal organisations. They open accounts with every single bank and launder money via small businesses. Usually, they do not wave a red flag and say, 'Look at me, I am high risk'. Often, they take over small businesses which were previously legitimate. It is very difficult to identify that any change has happened. The smart criminals always act under the thresholds, which makes them hard to detect. TMNL allows the banks to see whether a client has accounts with many different banks or whether there is evidence of suspicious withdrawals or deposits.

An industry speaker noted that obliged entities need to work together and cooperate on KYC and Know Your

Transaction (KYT) frameworks, which raises some privacy concerns. Obligated entities will have to cooperate more intensively with FIUs to avoid overwhelming them with an extremely high volume of suspicious transactions reports. A failure to report could be a criminal offence, but there are no sanctions for over reporting. This demonstrates why there is a need for obliged entities and competent authorities (incl. FIUs) to work together on intelligence led monitoring, exchanging information and receiving feedback. This also raises some privacy concerns.

An industry representative considered that the concerns around data privacy are understandable. Ultimately, society will have to make this decision. If banks are only allowed to see their own transactions, it will never be possible to compete with the bad actors. It is extremely important for banks and other institutions to be able to share data in an anonymous way.

5.3 Data protection rules can contribute to cost efficient and effective data collection

A regulator emphasised that the application of privacy rules can make the AML framework more efficient. There are synergies between the different sets of rules. The General Data Protection Regulation (GDPR) contains rules on data accuracy, which is crucial to the efforts of supervisors and obliged entities in detecting financial crime. Data minimisation is another key principle of GDPR. Supervisors should only collect the minimum level of data that is needed to monitor and carry out checks. This can also lower the administrative burden for obliged entities. In the last months, CNIL and the European Data Protection Board (EDPB) have expressed various public positions on the AML package. Data protection rules can be used to prevent obliged entities from de-risking by submitting false positives to FIUs without regard to the efficiency and effectiveness of their submissions.

5.4 Technology can foster privacy and assist in the monitoring and analysis of bulk data

An industry speaker highlighted the role of privacy enhancing technologies (PETs), such as data obfuscation tools, federated or distributed analytics, data accountability tools and encrypted data processing tools. These technologies allow for the processing, monitoring, and analysis of massive amounts of data without publishing the underlying private data or allowing the data processor to access any private data. However, these technologies will need more time to develop. Some of them are still in their infancy, others lack scalability or compatibility with other applications, and many require a massive amount of computational power and regular cleaning of data. Obligated entities

will have to design these tools and technologies into their transaction monitoring systems. These entities will have to adapt their procedures and processes, test them regularly, train their staff to understand them and perform privacy assessments.

The AML regulatory framework and the data protection regulatory environment are two different worlds with two different philosophies, concepts, and languages. Specialists in one domain are not always versed in the other. There must be a reconciliation between these worlds. Both domains need to work with each other on a common literacy that would bridge concepts to close this gap or at least move closer together.

5.5 Balancing effective AML and data protection in the digital euro

A regulator stated that the digital euro is an interesting example of the interplay between privacy and anti money laundering/countering the financing of terrorism (AML/CFT). The digital euro is an emerging technology with a social dimension. The Commission's text on the digital euro is now being discussed by the co legislators. In parallel, the ECB has launched a project to design the digital euro. There are two modalities for the digital euro: the offline modality with transactions on wallets and the online modality with transactions via account.

Privacy is the key condition for the success of the digital euro. In the ECB consultation in 2021, 43% of respondents highlighted confidentiality as the most important feature. In a very competitive payment landscape, in which private payments work well, the EDPB believes that the value added of the digital euro is confidentiality and privacy. To generate public trust in the project, there will need to be a parallel with physical cash. Privacy by design will be crucial to the success of the digital euro.

The offline modality, which was introduced by the recent Commission text, is a point of satisfaction for data protection authorities. It does not allow AML transaction monitoring for small value and proximity transactions. This is equivalent to cash. CNIL believes that this monitoring is not needed. Offline transactions do not need to be subject to transaction monitoring because they are low risk. The EDPB is in favour of applying this approach to online transactions on account, as well, which the Commission proposal does not do. The AML risk can be mitigated in the design phase to ensure that this a low risk activity or that low value online transactions have the same level of AML risk as those conducted with physical cash. A proper assessment of the interplay between both sets of policy objectives during the design phase of the digital euro will lead to greater technological possibilities and increased social acceptability.