Linklaters

AMLD6, AMLR & AMLA: a new anti-money laundering era in the EU

April 2024

With its approval by the EU Parliament, the anti-money laundering (AML) and counter terrorist financing (CFT) package is almost final. It is a big step forward in terms of harmonisation and will bring a new EU authority.

Few legislative initiatives have such a broad impact: all financial institutions and many non-financial companies must comply with AML/CFT requirements and failing to do so exposes in-scope companies to significant fines and strict enforcement.

Main aspects of the AML/CFT package

What's in it?

The first anti-money laundering Directive was adopted in 1990 to prevent the misuse of the financial system for the purpose of money laundering. Since then, it has been gradually expanded and developed, but always left considerable leeway to the Member States.

In terms of material obligations, the new AML/CFT package will be just a further step in this long chain of legislation. It includes:

> a **new regulation** (**AMLR**) to replace and enhance the requirements of the Directive (EU) 2015/849, especially for customer due diligence (CDD),

> a **new directive** (**AMLD6**) to replace and modify the remaining parts of Directive (EU) 2015/849, and

> a new regulation to establish the **new European Anti-Money Laundering Authority** (**AMLA**).

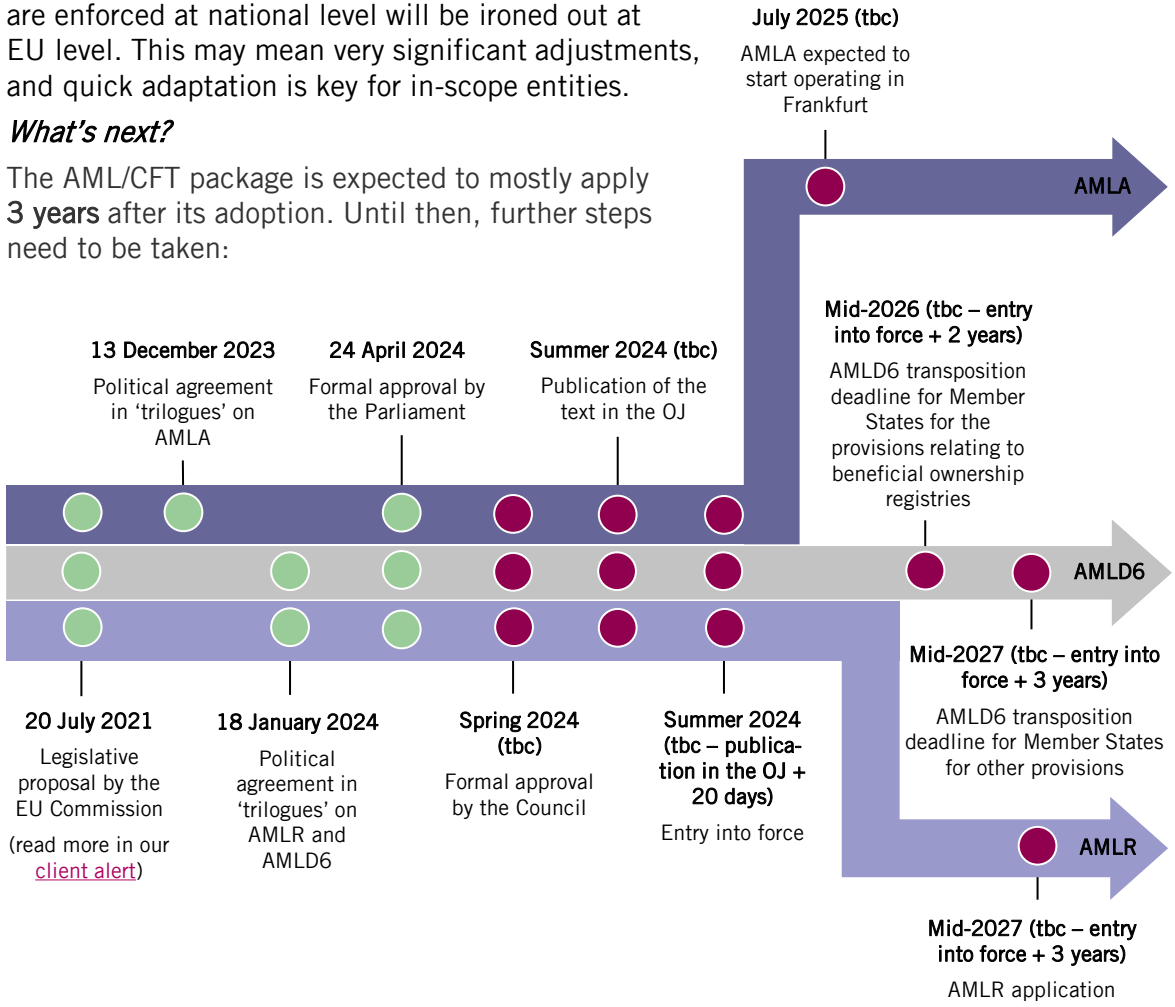
The package contains significant fine-tuning and incremental changes, but no fundamental shifts. Yet, it is worth noting that the AMLR will be the first directly applicable piece of legislation in this area of law. It also covers some of the most important aspects of the AML regime. The **highest degree of harmonisation enters an area where national idiosyncrasies are commonplace**. This is topped by the new AMLA, which will be responsible for promoting supervisory convergence.

As a result, **the real revolution is the mindset shift** that both supervisors and legal practitioners will experience.

The little (or big) differences on how some concepts are enforced at national level will be ironed out at EU level. This may mean very significant adjustments, and quick adaptation is key for in-scope entities.

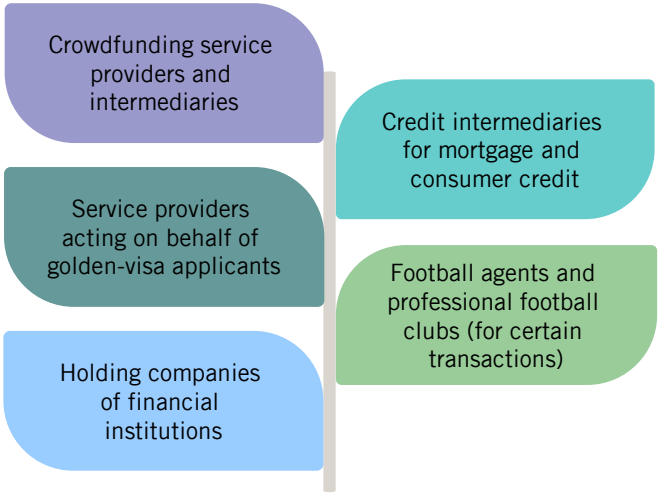
What's next?

The AML/CFT package is expected to mostly apply **3 years** after its adoption. Until then, further steps need to be taken:



Expanded scope

Most defined terms remain consistent with those established in the current AMLD5. However, there have been some additions to the list of obliged entities:



There are also a few amendments to the existing terms:

> In-scope crypto-asset service providers (**CASPs**) are defined by reference to the **MiCA Regulation**. The AMLR therefore covers a wider set of players than the AMLD5 and potentially supersedes existing CASP registries.

> The rather vague definition of "**traders in goods**" has been replaced by more concrete definitions, including the trade, storage or intermediation in the trade of **cultural goods** (such as pieces of art), **precious metals** and stones and certain **high-value goods**, including planes, boats and motor vehicles.

Cross-border activity within the EU

The new general rule is that the obliged entity must comply with the requirements of the host Member State where it has a **subsidiary**, a **branch**, **agents**, **distributors** or **other types of infrastructure**. Certain types of intermediaries (electronic money issuers, payment service providers, CASPs) may instead comply with the requirements of their home Member State based on criteria to be set in future regulatory technical standards (RTS).

This leaves **pure remote cross-border operations** with no infrastructure, subject to home Member State requirements only. However, caution is advised as the AMLR allows for certain exceptions under national law and much depends on the interpretation of the concept of infrastructure.

Additionally, a new kind of **EU passport** procedure is introduced. Obliged entities must notify their AML supervisors if they intend to carry out activities in another Member State. The supervisor, in response, will communicate with the host Member State's AML supervisor. An entity must send a notification as soon as it takes steps towards acting cross-border and, in case of branches, at least 3 months in advance.

Obliged entities subject to **specific passport notification procedures** under other EU laws (e.g. MiFID or CRD) are exempted from this requirement.

No passport or equivalence is provided for **third-country-based** obliged entities.

> An expanded list of obliged entities is supplemented with clearer rules on home-host distribution of AML/CFT-requirements within the EU.
>
> This is expected to harmonise criteria on when local compliance is required. Cross-border groups will have a clearer view of their obligations.

Customer Due Diligence (CDD)

Changes to the scope of the CDD obligation

> The AMLR lowers the threshold for CDD obligations regarding occasional transactions from EUR 15,000 (under AMLD5) to EUR 10,000. Additionally, the AMLR introduces new thresholds for occasional transactions of CASPs (EUR 1,000) and for cash transactions (EUR 3,000).

> CDD will also cover services related to the participation in the creation or transfer of ownership of legal entities or arrangements.

> CDD measures should be implemented if it is unclear whether the appearing person is the actual customer, or if they act on behalf of others.

> AMLA is mandated to develop RTS specifying entities, sectors, or transactions with higher risks and establishing related transaction thresholds.

Definition of customer

There is still no general definition of "customer" for the purposes of CDD. However, the AMLR does provide indications for 3 specific cases:

- For traders in goods, both the direct customer and the supplier are customers
- For lawyers and notaries, if they are the only ones intermediating, both parties are customers
- For real estate agents, both parties to the transaction are customers

Identification data

> The **information** that obliged entities need to obtain to identify the **customer and the beneficial owner** is now listed.

> Electronic means of **distance identification** will need to meet the requirements of the eIDAS Regulation with assurance levels "substantial" or "high".

> When customers use **virtual IBANs**, the bank or payment provider that receives the redirected payments must be able to get the user's identification details from the virtual IBAN provider within 5 working days.

> If verifying a beneficial owner's identity might alert the customer that the entity is suspicious (**tip off**), the obliged entities should not verify the senior managers' identities. Instead, they should document the measures taken to identify both the beneficial owners and senior managers.

> The frequency of **updating customer information** (ongoing monitoring of the business relationship) continues to be based on the risk of the relevant business relationship. However, it is now clarified that this must be done **at least every 5 years**.

> Specific rules on **simplified and enhanced due diligence** are now listed directly in the AMLR.

Two aspects are particularly worth noting:

> The CDD obligations are now directly applicable as part of the AMLR, which leads to much less room for divergence at national level.

> AMLA will develop RTS to specify and harmonise various CDD aspects. We expect them to be key in day-to-day compliance.

Reliance and outsourcing

The new rules clarify the respective conditions for **reliance on CDD** already performed by other obliged entities and regulates the outsourcing of functions.

A **risk-based approach** must be applied, especially in cases where providers are based in high-risk third countries. The ultimate responsibility for conformity with the rules remains with the obliged entity. Obliged entities must **notify their supervisor of the outsourcing** in advance.

The following tasks cannot be outsourced under any circumstances:

> proposal and approval of the obliged entity's **business-wide risk assessment**;

> approval of the obliged entity's **policies**, controls and procedures;

> decisions on the **risk profile** to be attributed to the customer;

> decisions to **enter into a business relationship** or **carry out an occasional transaction** with a client;

> the **reporting to FIUs** (financial intelligence units) **of suspicious activities** or threshold-based reports, except where such activities are outsourced to another obliged entity in the same group which is established in the same Member State; and

> the approval of the **criteria for the detection** of suspicious or unusual transactions and activities.

Third-country policy

The approach towards **third countries** is adapted. The EU Commission will identify third countries that will be subject to different sets of measures, proportionate to the risk they pose to the Union's financial system:

> **High-risk third countries**: Third countries subject to a call for action by the FATF. Due to the persistent strategic deficiencies in their AML/CFT framework, they will be subject to all enhanced due diligence measures, as well as country-specific countermeasures to proportionately mitigate the threat.

> **Third countries with compliance weaknesses**: Those subject to increased monitoring by the FATF. They will be subject to country-specific enhanced due diligence measures proportionate to the risks.

> **Third countries posing a specific and serious threat**: Countries that, although not listed by the FATF, are identified by the EU Commission as problematic. Based on that threat, they will be subject either to country-specific enhanced due diligence measures or to all enhanced due diligence measures and counter-measures. The EU Commission will leverage AMLA's technical expertise to define threat levels.

Back to top

Information registers

A cornerstone of the new rules is the collection and dissemination of information which can be used to prevent ML/TF. Several databases and repositories are created/ expanded which the different authorities, supervisors, obliged entities and other persons with legitimate interest can access to prevent ML/TF more effectively.

The level of access, the process and the use of the information is subject to detailed rules which seek to ensure the adequacy and accuracy of the information together with the appropriate degree of privacy and data protection.

Bank account register

In each Member State, a centralised automated mechanism, such as a central register or central electronic data retrieval system, will exist and will allow the identification of any natural or legal person holding or controlling:

> **payment accounts** or **bank accounts** identified by IBAN, including virtual IBANs;

> **securities accounts**;

> **custodial crypto-asset accounts**; and

> **safe-deposit boxes** held by a credit or financial institution.

This information will be accessible to FIUs, the AMLA and supervisory authorities. The EU Commission may adopt implementing acts establishing the format for the submission of the information to these registers.

Real estate register

Member States will provide a single access point for the swift identification of any land or real estate property. It will include information on the natural persons or legal entities owning that property, as well as information allowing the identification and analysis of related transactions. Competent authorities and the AMLA will be able to access it in the framework of their supervision.

Central AML/CFT database

AMLA will establish and keep up to date a central database of information collected in the pursuit of its activities. It will be made available, on a need-to-know and confidential basis, to national and EU supervisory authorities.

The database will, inter alia, include a list of all supervisory authorities, statistical information and administrative measures taken as well as pecuniary sanctions imposed.

Back to top

Beneficial ownership register

AMLD6 introduces further enhancements to the central beneficial ownership registers in each Member State.

Content

The registers will contain information on the **beneficial owners** of legal entities, trusts or similar arrangements and nominee arrangements with respect to nominee shareholders and nominee directors of legal entities.

Where **no person is identified as beneficial owner**, the central register will include (i) a statement that no beneficial owner exists, or could not be identified and the reasons why, and (ii) the details of all natural persons who hold the position of senior managing official(s) in the legal entity.

The registers will also include an indication on whether listed legal entities and legal arrangements are associated with persons subject to **financial sanctions**.

New obligations to file information

The new rules also place obligations on **nominee shareholders and directors** to maintain and disclose information on their nominators and beneficial owners.

Previously limited to trusts, now also other types of **third-country legal entities and arrangements that enter into business relationships within the EU** or acquire real estate must submit beneficial ownership information. More clarity is provided on the exact scope and triggers of this obligation.

Changes to the definition of beneficial owner

While the general obligation to identify beneficial owners remains basically the same, the AMLR has elaborated on many important points:

> The threshold for beneficial ownership through ownership interest will remain at **25%**. However, the AMLR empowers the EU Commission to set **lower thresholds** via a delegated act for specific high-risk categories of entities. Calculation methods for complex ownership structures are clarified.

> The AMLR also provides a more detailed definition of beneficial owners of a **trust** and what information trustees must keep. The new legislation clarifies definitions and expands the scope of the previous directive. For instance, it includes rules on other **legal arrangements similar to trusts**.

> It also clarifies how to act in specific cases: e.g., (i) when beneficiaries of a legal entity are not yet determined, (ii) when there is a default beneficiary, or (iii) beneficial owners in an investment fund.

> A mechanism is established to deal with **inconsistent data.** Errors or inaccurate information will need to be reported when detected.

> The information about beneficial ownership will be available through the national registers for at least **5 years**, and no more than **10 years** after the legal entity has been deleted from the register.

Back to top

Compliance policies and procedures

Prior AML legislation already included a requirement to have a ML/TF prevention policy in place, and duly comply with it. On a risk-based approach, obliged entities had to identify, assess and mitigate risks.

The relevant rules are now included in the AMLR which is **directly applicable**, without the filter of national implementation. We expect that in practice a more homogeneous approach will be feasible, which will help transnational groups to have more coherent group-wide policies.

Some new developments include:

> Obliged entities must take measures at management level to implement internal policies, controls and procedures, including the appointment of **new dedicated roles.** In particular, they must have both:

  i. a **compliance manager**, who must be an executive member of the board of directors (or an equivalent governing body) responsible for the implementation of AML/CFT policies, controls and procedures and for receiving information on significant or material weaknesses; and

  ii. a **compliance officer**, in charge of the day-to-day operation of the AML/CFT policies, contact point for competent authorities and responsible for reporting suspicious transactions to the FIU.

  Where the nature, risk, size and complexity of the relevant entity's business justify it, the functions of both roles may be performed by the same individual.

> The risk assessment, now called **business-wide risk assessment**, must take into account not only the nature and size of the obliged entity, but also the nature of its business, including its risk and complexity.

In addition, more clarity is provided for group-level situations:

> Compliance functions must be established at **group level**. They must in any case include a compliance manager at group level and, where appropriate, a group compliance officer.

> **Sharing of information** within a group shall cover e.g. the customer's identity, beneficial owners, the nature and purpose of the business relationship and suspicions reported to the FIU.

> RTS will further elaborate on **minimum group-wide policy requirements**, the role and responsibilities of parent companies that are not themselves obliged entities, and the conditions under which other structures such as networks and partnerships should apply group-wide measures.

AML policies and compliance functions will need to be adapted.

Emphasis is put on group-wide requirements which we expect to become more easily translatable from one Member State to another.

Level 2 legislation will clarify and develop the distribution of responsibilities at group level.

Obliged entity reporting obligations

The scope of suspicious transaction reporting remains consistent with established practices. A **deadline of 5 working days** is now included to respond to FIU follow-up requests, which may be shortened in urgent cases.

Obliged entities must assess their customers' transactions or activities against any relevant information they possess, prioritising based on urgency and risks. Suspicions are based on various factors, including **customer characteristics**, **transaction size and nature, patterns**, **fund origins** and **destination** or any other known circumstance, including the client's risk profile.

AMLA will develop **implementing technical standards for the format** of reporting suspicions and transaction records and will also provide guidance on indicators of suspicious activity or behaviours.

The **tipping off prohibition** is kept in force in similar terms as stipulated in AMLD5.

New reporting obligations are created for specific transactions on certain **high-value goods**, including motor vehicles above EUR 250,000, and ships and airplanes above EUR 7,500,000.

Risk assessments and reports

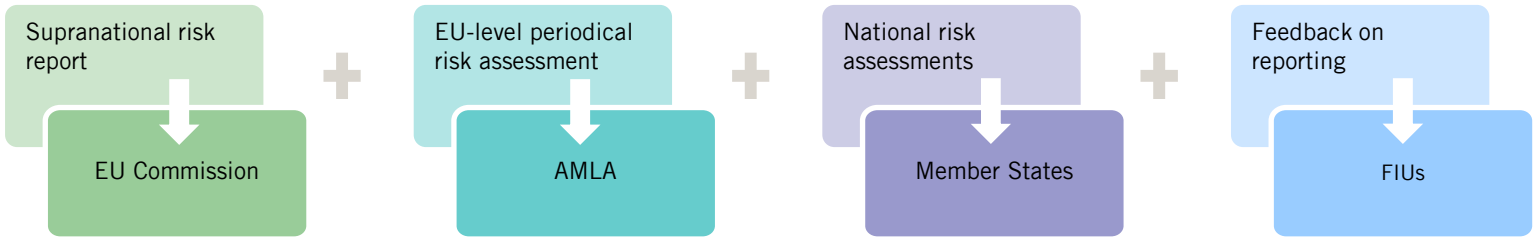
Different public authorities will be mandated to issue reports, which may be a useful tool for compliance.

> The Commission will prepare a **supranational risk assessment report**, follow-up reports and an analysis on the works of beneficial ownership registers.

> AMLA will prepare periodical reports on **EU-level risks**, along with its general power to issue level 3 documents, such as guidelines and opinions.

> Member States will have to provide **national risk assessment reports** and will also need to report on risks associated with golden-visa programmes.

Interestingly, along with annual reports, FIUs will also have to provide **feedback to obliged entities** on the reporting of suspected ML/TF at least once a year.



Anonymous instruments

Financial institutions and crypto-asset service providers may not keep **anonymous accounts**, including bank accounts, payment accounts, passbooks, safe deposit boxes, and crypto-asset custody accounts. Existing anonymous accounts must undergo CDD before being used in any way.

Non-listed companies are banned from issuing **bearer shares**. All existing bearer shares must be converted into registered shares, immobilised or deposited with a financial institution within 2 years after the AMLR comes into effect. If not converted within this timeframe, their associated rights, including voting and distribution rights, will be suspended until compliance is achieved. After 3 years, non-compliant shares will be cancelled, resulting in a decrease in share capital.

Traders in goods or services cannot accept **cash payments** of over EUR 10,000 for a single purchase. Member States may adopt lower limits for cash transactions or keep their existing ones. This limit does not apply to private transactions between individuals, or to payments made at financial institutions who will instead need to report them to the FIU.

Politically exposed persons (PEPs)

In general, the provisions on PEPs are based on the AMLD5. However, there is a new obligation relating to persons who no longer hold prominent public functions. Obliged entities must apply certain enhanced CDD measures to them as laid down in the AMLR.

The AMLA will issue guidelines on:

> the criteria for the identification of persons known to be a **close associate** of a PEP, and

> the level of risk associated with **particular categories of PEPs**, their family members or persons known to be close associates, and how such risks are to be assessed after the person no longer holds a prominent public function.

Data protection and processing

As was the case so far, obliged entities are permitted to process special GDPR categories of personal data and data relating to criminal convictions and offences when strictly necessary for ML/TF prevention. No commercial or other use is permitted. The AMLR develops further the specific safeguards that they must adhere to:

> They must **inform** (prospective) customers that the data may be processed to comply with AML/CFT regulations, ensure that data come from **reliable sources** and are accurate and current, **avoid biased and discriminatory decisions** based on that data, and implement security measures for data confidentiality.

> When processing personal data, they must distinguish between **allegations**, **investigations**, **proceedings**, and **convictions**, respecting the right to a fair trial and the presumption of innocence.

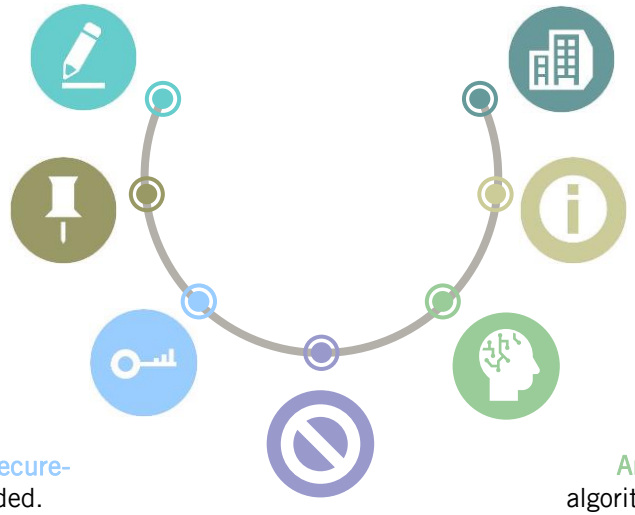
> They may use **automated decision-making** processes, but only with data obtained as part of their CDD obligations. Any decisions made by these systems must involve meaningful human intervention to ensure accuracy and appropriateness. Customers affected by these decisions have the right to an explanation and the ability to challenge the decisions, except for suspicious transaction reports.

Information sharing partnerships

As a new significant development, the AMLR allows information-sharing partnerships, i.e., groups of obliged entities that share information to comply with their AML/CFT obligations.

Obliged entities looking to join such partnerships must notify their AML supervisory authorities, which will verify the partnerships' compliance mechanisms and ensure that a data protection impact assessment has been conducted. The responsibility for compliance with the law remains with the partnership participants.

Competent authorities may participate in information sharing partnerships only for the exchange of information necessary for their tasks, and those with enforcement functions must follow national law, including judicial authorisation where needed.



Information exchange within these partnerships is limited to customer information, transaction details, risk factors, and ML/TF suspicions. Partnerships may designate a single entity to file reports to FIUs on suspicious activities discovered through them.

Obliged entities in these partnerships must establish internal policies for information sharing, defining the scope, roles and risk assessments to determine when higher-risk information can be shared. These procedures should be established before joining the partnership.

Information should be shared securely, and access must be recorded. Sharing is limited to cases involving high-risk customers or those requiring additional scrutiny.

Information received in the partnership should not be transmitted further, except to the authorities if required.

Artificial intelligence or algorithm-generated information must have adequate human oversight before sharing.

> Information-sharing partnerships may help both obliged entities and supervisors to comply with their respective AML/CFT obligations more efficiently. They provide a regulated and supervised way to share relevant information to supplement one's own CDD analysis.

AMLA

AMLA is the new regulatory authority for AML/CFT and will assist national authorities in increasing their effectiveness. It has **two main roles**:

> ensuring a high-quality supervision; and

> contributing to supervisory convergence and a common supervisory culture.

Directly supervised entities

AMLA will directly supervise the **riskiest obliged entities** and groups of the financial sector and will monitor and ensure compliance with AML/CFT requirements of both the individual entities and associated groups.

The entities subject to AMLA's direct supervision will be **selected by the authority itself**, based on cross-border activity and a harmonised methodology using objective criteria centred on risk categorisation. AMLA will develop technical standards for determining the risk profile. These standards shall take into account the specificities of each sector. The selection process relies on data provided by national financial supervisors.

The first **selection process** is foreseen for mid-2027, starting with up to 40 supervised groups and entities. The list of selected entities will be reviewed every 3 years. Obliged entities remain under direct supervision for at least 3 years, even if they cease to meet the selection criteria during that time.

Furthermore, AMLA will also be able to request the Commission to be designated as the direct supervisor for **financial sector entities with specific systematic failures or particular risk profiles**. National supervisors may also ask AMLA to take over the supervision of an obliged entity.

Supervisory actions

To ensure compliance with the regulatory AML framework, AMLA can conduct supervisory reviews and assessments on individual entities and at group-wide level to determine whether the internal policies, procedures and controls put in place are adequate.

AMLA's competences vis-à-vis the directly supervised obliged entities include:

> requiring entities, natural or legal persons, and third parties to whom operational functions are outsourced, to provide necessary **information**;

> conducting all necessary **investigations** of any obliged entity, including the power to request the submission of documents;

> conducting all necessary on-site **inspections** at the business premises of the natural and legal persons;

> imposing **administrative measures**, e.g., require to reinforce internal procedures or changes in governance structure; and

> imposing **fines**.

National supervisors

AMLA's other main responsibility is to supervise the **national financial supervisors** (e.g. securities market and banking authorities). AMLA will carry out periodic assessments to ensure they have adequate resources and powers for the implementation of AML/CFT measures.

In addition, AMLA shall contribute – in collaboration with the national financial supervisors – to the **convergence of supervisory practices** and promotion of high AML/CFT supervisory standards. In this regard, AMLA shall develop new practical instruments and convergence tools to promote common supervisory approaches and best practices.

AMLA must provide **assistance** requested by national supervisors. In case of disputes between national financial supervisors AMLA acts as a **mediator**. For that purpose, AMLA may settle, with binding effect, disagreements concerning measures to be taken with regard to an obliged entity. AMLA has similar obligations regarding non-financial supervisors.

Financial Intelligence Units (FIUs)

AMLA shall also foster the cooperation between FIUs and **support and coordinate their work**. It may identify and select relevant ML/TF cases for the joint analyses by FIUs. In case of disagreements between FIUs, AMLA shall further act as a mediator and has the duty to develop tools and services to enhance their capabilities.

AMLA may **request non-operational data and analyses** from FIUs where they are necessary for the assessment of ML/TF threats, vulnerabilities and risks facing the internal market and may collect information and statistics regarding the FIUs' tasks and activities.

Structure

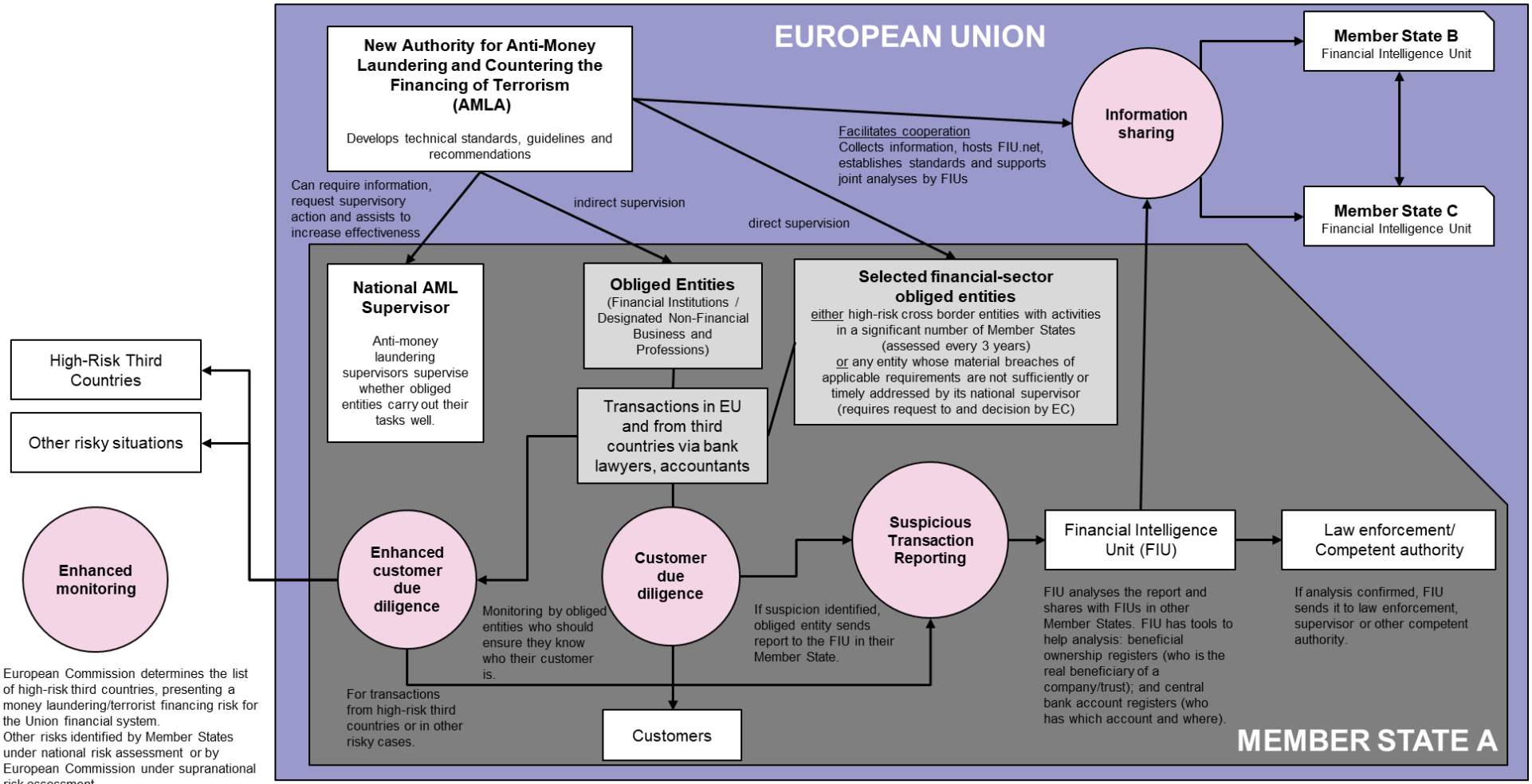
AMLA will have a Chair and an Executive Director.

> The **Chair** will represent AMLA and presides over the two collegial governing bodies, the Executive and the General Board. The General Board will adopt all regulatory instruments such as technical standards, and the Executive Board will be in charge of decisions towards individual obliged entities or supervisory authorities.

> The **Executive Director** will oversee the day-to-day management and budget implementation, resources, staff and procurement.

The future will show how AMLA and its power to develop technical standards and issue guidance for all obliged entities, national supervisors and FIUs will affect and shape the national supervision of obliged entities across all relevant sectors. National guidance will continue to apply until it is replaced by guidance at EU level.

Preventing money laundering and terrorist financing across the EU - How will it work in practice?



Source: Graphic based on graphic provided by EC

Key contacts

Andreas Dehio
FRG Partner, Frankfurt
Tel: +49 69 71003 583
andreas.dehio@linklaters.com

Etienne Dessy
FRG Partner, Brussels
Tel: +32 2 501 9069
etienne.dessy@linklaters.com

Paloma Fierro
FRG Partner, Madrid
Tel: +34 91399 6054
paloma.fierro@linklaters.com

Raoul Heinen
Funds Partner, Luxembourg
Tel: +35 22608 8331
raoul.heinen@linklaters.com

Bas Jennen
FRG Partner, Amsterdam
Tel: +31 207996 287
bas.jennen@linklaters.com

Stefaan Loosveld
LAI Partner, Brussels
Tel: +32 2 501 9521
stefaan.loosveld@linklaters.com

Ngoc-Hong Ma
FRG Partner, Paris
Tel: +33 15643 5893
ngoc-hong.ma@linklaters.com

Christian Schmitt
LAI Partner, Frankfurt
Tel: +49 69 71003 261
christian.schmitt@linklaters.com

Kerstin Wilhelm
LAI Partner, Munich
Tel: +49 89 41808 506
kerstin.wilhelm@linklaters.com

Anna Ferraresso
Finance Counsel, Milan
Tel: +39 0288393 5257
anna.ferraresso@linklaters.com

Vera Ferreira de Lima
FRG Counsel, Lisbon
Tel: +35 1218640 091
vera.lima@linklaters.com

linklaters.com