TRANSPARENCY INTERNATIONAL EU

European Union's legislative framework on obliged entities

March 2026

ABOUT THIS SERIES OF EXPLANATORY DOCUMENTS

This document forms part of a series of five thematic legislative assessments covering crypto-assets, real estate, beneficial ownership, Financial Intelligence Units (FIUs), and obliged entities. The series has been prepared by Transparency International EU at the request of BIRN Albania and provides an overview of key developments introduced under the European Union's AML (Anti-Money Laundering) package adopted in 2024. It presents the original legal provisions which are accompanied by an explainers and examples of good practices identified by Transparency International through its reports, with the aim of supporting better understanding and implementation.

This is the original English version of the comparative analysis.To promote inclusive and informed engagement, the documents have also been translated into Albanian (Link). These translations are intended to support civil society organizations, academic institutions, investigative journalists, and other stakeholders in participating effectively in consultations and reform processes related to transparency and financial integrity.

These documents are intended for informational and analytical purposes only. They do not constitute legal advice, nor do they represent an official interpretation of European Union law.

SUMMARY OF THE EU AML INSTITUTIONAL FRAMEWORK: OBLIGED ENTITIES

The Sixth Anti-Money Laundering Regulation (AMLR6) establishes a uniform legal framework across the Union, providing directly applicable rules designed to eliminate the fragmentation caused by varying national implementations. AMLR6 identified obliged entities as the essential gatekeepers of the Union's financial system, legally responsible for identifying, mitigating, and managing the risks of money laundering and terrorist financing. By clearly defining the internal structures and professional relationships required of these actors, the framework ensures a consistent understanding of the legal environment in which they must operate to prevent illicit financial flows.

In parallel, the Sixth Anti-Money Laundering Directive (AMLD6) defines the mechanisms to be put in place by Member States to underpin this institutional framework. It introduces 'fit and proper' checks, requiring supervisors to verify the honesty, integrity, and expertise of senior management and beneficial owners of obliged entities. Furthermore, the AMLD6 transforms the national risk assessment into a strategic tool, requiring Member States to share findings with the private sector to help obliged entities tailor their internal checks to the specific areas where the danger of illicit activity is highest.

To lead and coordinate these efforts, the AMLA Regulation establishes the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). To lead and coordinate these efforts, the AMLA Regulation establishes the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Its core mandate is to safeguard the public interest and uphold the integrity of the Union's financial system by ensuring high-quality supervision and contributing to supervisory convergence across the internal market. AMLA serves as the centre of an integrated AML/CFT supervisory system, bringing together the Authority and national supervisory authorities composed of the AMLA itself and national supervisory authorities working in good faith, cooperation and consistent application of Union rules.

This integrated system operates through a dual mechanism of oversight. For selected obliged entities, high-risk financial institutions operating in at least six Member States, the AMLA exercises direct supervision. These obliged entities are overseen by Joint Supervisory Teams led by AMLA. For non-selected obliged entities, supervision remains at the national level, but under the indirect oversight of the AMLA to ensure that supervisory practices are consistent and of a high quality across the Union.

To support this unified approach, AMLA is tasked with developing a harmonised AML/CFT supervisory methodology that applies a risk-based approach to all obliged entities in the Union. This methodology is supported by a central AML/CFT database, which tracks the risk profiles, compliance history, and administrative sanctions of individual entities to identify systemic vulnerabilities. To ensure the sustainability and independence of this specialised oversight, the system is funded by annual supervisory fees levied on the most complex and risky obliged entities, ensuring the burden of regulation remains proportionate to the risk each entity poses to the internal market.

AML REGULATION, "THE SINGLE REGULATORY FRAMEWORK"

RELEVANT LEGISLATION

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31st May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (known as the "single rulebook")

PROVISIONS	EXPLAINER
Subject matter and definitions Section 1 – Chapter I	These Articles establish a **uniform legal framework** across the Union to ensure that the financial system is not misused for criminal purposes. By providing direct applicability of rules, **it aims to eliminate the fragmentation caused by varying national implementations.** To achieve this, it defines the specific professional actors, known as gatekeepers, who are responsible for identifying and mitigating risks. By clearly defining what constitutes a professional relationship and the internal structures of these entities, the Regulation ensures that all designated parties have a consistent understanding of their role and the legal environment in which they must operate to prevent illicit financial flows.
Article 1 This Regulation lays down rules concerning: (a) The **measures to be applied by obliged entities to prevent money laundering and terrorist financing**	
Article 2 1) For the purposes of this Regulation, the following definitions apply: (18) **'establishment'** means the actual pursuit by an obliged entity of an economic activity (…) (19) **'business relationship'** means a business, professional or commercial relationship connected with the professional activities of an obliged entity, which is set up between an obliged entity and a customer (…)	

(37) **'management body'** means an obliged entity's body (…), which are empowered to set (…) strategy, objectives and overall direction, and which oversee and monitor management decision-making, and include the persons who effectively direct the business of the obliged entity; where no such body exists, the person who effectively directs the business of the obliged entity; (42) **'parent undertakings'** means: (b) for groups whose head office is located outside of the Union, where at least two subsidiary undertakings are obliged entities established in the Union, an undertaking within that group established in the Union (…) (45) **'supervisor'** means the body entrusted with responsibilities aimed at ensuring compliance by obliged entities (57) **'partnership for information sharing'** means a mechanism that enables the sharing and processing of information between obliged entities and (...) competent authorities	
Obliged entities Article 3	This article provides a list of entities considered to be OE; the list provided in this table is non-exhaustive.
The following entities are to be considered obliged entities for the purposes of this Regulation: (1) Credit institutions; (2) Financial institutions; etc	

Notifications of cross-border operations and application of national law Article 8	
1) Obliged entities wishing to carry out activities within the territory of another Member State for the first time shall **notify the supervisors** of their home Member State of the activities which they intend to carry out in that other Member State. (…) The first subparagraph shall not apply to obliged entities subject to specific notification procedure. 3) (…) **obliged entities shall comply with the national rules** of the Member State in which they are established. 4) Where obliged entities operate establishments in several Member States, they shall ensure that each establishment applies the rules of the Member State in which it is located. 5) Where obliged entities (…) operate (…) through agents, distributors, or though other types of infrastructure (…) they shall apply the rules of the Member States in which they provide services	When **obliged entities** exercise their freedom to provide services or establish themselves in different countries within the Union, they **must notify their home authorities**. To address specific local risks and maintain the integrity of the internal market, these entities are **required to follow the specific anti-money laundering requirements of the country where they actually conduct their economic activity** or maintain a stable infrastructure. This **prevents the use of "letter-box" entities to bypass regulations** and ensures that wherever an entity operates, it is held accountable to the standards designed to protect that specific jurisdiction.

Scope of internal policies, procedures and controls Article 9	Every **obliged entity must build a custom internal 'defence manual' that scales with its size and complexity**. This includes not only setting the rules for customer checks and reporting but also having an independent person or department audit those rules to make sure they actually work.
1) Obliged entities shall have in place internal policies, procedures and controls in order to ensure compliance (…) and in particular: (a) mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entities (…) 2) The policies (…) shall include: (i) the carrying out and updating of the business-wide risk assessment (ii) the obliged entity's risk management framework (…) (b) internal controls and an independent audit function to test the internal policies and procedures (…) in absence of an independent audit function, obliged entities may have this test carried out by an external expert. 3) (…) 4) By 10 July 2026, AMLA shall issue guidelines on the elements that obliged entities should take into account (…) when deciding on the extent of their internal policies, procedures and controls.	

Business-wide risk assessment Article 10	Obliged entities must actively identify, asses, and maintain a clear understanding of **specific risks** they face across their business. This document must be update whenever the business changes or new threats emerge.
1) Obliged entities shall take appropriate measures (…) to identify updates the risks of money laundering and terrorist financing to which they are exposed (…) 2) The business-wide risk assessment (…) shall be documented, kept up-to date and regulatory reviewed (…). It shall be made available to supervisors upon request.	
Article 11-14	A **senior manager must oversee the overall strategy and resources,** while a dedicated compliance officer manages the daily technical tasks and serves as the primary contact for LEAs and regulators. **Obliged entities must ensure that their staff**, as well as external representatives like agents, are not only **well-trained in recognizing suspicious patterns** but also **possess the necessary expertise and professional integrity.** To protect the system from internal vulnerabilities, entities must actively manage potential conflict of interest, especially when employees have personal ties to clients that could influence their judgment. N.B.: Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law.
Article 11 1) Obliged entities shall appoint one member of the management body (…) responsible for ensuring compliance with this Regulation (…). 2) Obliged entities shall have a compliance officer (…) responsible for the policies, procedures and controls in the day-to-day operation. **Article 12** (…) **Obliged entities shall take measures to ensure** that their **employees** (…) including their agents and distributors **are aware of the requirements arising from this Regulation** (…) in specific, ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing (…).	

Article 13 1) Any employee (…) directly participating in the obliged entity's compliance (…) shall undergo an assessment (…) of: (a) individual skills, knowledge and expertise to carry out their functions effectively. (b) good repute, honesty and integrity 2) **Employees** (…) **shall inform the compliance officer of any close private or professional relationship established with the obliged entity's customers** or prospective customers and shall be prevented from undertaking any tasks related to the obliged entity's compliance in relation to those customers. 3) Obliged entities shall have in place procedures to prevent and manage conflicts of interest (….) **Article 14** 2) Obliged entities shall establish internal reporting channels that meet the requirements set out in Directive (EU) 2019/1937.	

Article 16-17	
Article 16 1) (…) **Obliged entities** (…) shall **implement those group-wide policies, procedures and controls**, taking into account their specificities and the risks to which they are exposed. 2) (…) the compliance manager shall submit once a year a report on the implementation of the obliged entity's internal policies, procedures and controls (…) 3) The **policies, procedures and controls** pertaining to the sharing of information (…) shall **require obliged entities** (…) to **exchange information** when such sharing is relevant for the purposes of customer due diligence (…). 4) By 10 July 2026, AMLA shall develop draft regulatory standards to specify minimum requirements of group-wide policies (procedures and controls), and submit them to the Commission for adoption **Article 17** 1) **Where branches or subsidiaries of obliged entities are located in third countries where the minimum AML/CFR requirements are less strict** (…) the **parent undertaking shall ensure that those branches or subsidiaries comply** (…) **with this Regulation.** 3) By 10 July 2026, **AMLA shall develop draft regulatory technical standards** and submit them to the Commission. (…) [this draft] shall [include] the minimum action to be taken by obliged entities where the law of a third country does not permit the implementation of the measures required under Article 16 (…).	The obliged entity is responsible **for ensuring that every part of its organisation follows the same high standards for risk assessment** and information sharing. This is particularly vital when operating in countries with weaker laws; in such cases, the group must apply EU-level protections to prevent its international network from becoming a weak link that criminals can exploit. Where the law of a third country does not permit compliance with the Regulation, the parent company shall take additional measures to ensure that branches and subsidiaries in that third country effectively handles the risk of money laundering. This may include closing operations to protect the integrity of the Union's financial system.

Outsourcing Article 18	
1) Obliged entities may outsource tasks resulting from this Regulation to service providers. The obliged entity shall notify the supervisor of the outsourcing before the service provider starts to carry out the outsourced task. 2) The obliged entity shall remain fully liable for any action (…) connected to the outsourced tasks (…) 3) (…) The following tasks **shall not be outsourced** tasks under any circumstances: (a) the proposal and approval of the obliged entity's nosiness-wide risk assessment (…) (b) the approval of the obliged entity's internal policies (…) (c) decision on the risk profile to be attributed to the customer; (d) the decision to enter into a business relationship or carry out an occasional transaction with a client (e) the reporting to FIU of suspicious activities (…) (f) the approval of the criteria for the detection of suspicious or unusual transactions and activities 4) (…) 5) 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.	While **gatekeepers** can hire external help for technical tasks or remote identification, they **can never "outsource their responsibility".** The entity remains legally accountable for any mistakes made by a service provider. Some functions are non-delegable, and they must remain under the direct control of the obliged entity.

Application of customer due diligence measures Article 19	Specific tripwires require a gatekeeper to verify who they are dealing with. This includes starting any long-term relationship or handling large one-off transactions. Certain activities are more attractive to criminals, the law sets lower thresholds for high-risks areas such as cash transactions which require checks at EUR 3 000, and gambling activities at EUR 2 000. **Regardless of the amount, any hint of suspicion or doubt about a client's identify immediately triggers a full investigation.**
1) **Obliged entities shall apply customer due diligence measures** (…) (a) **when establishing a business relationship**; (b) when carrying out an **occasional transaction** of a value of at least **EUR 100 000** (…) (d) when there is a **suspicion of money laundering** or terrorist financing (…) 4) (…) apply at least [identification] measures (…) when carrying out an **occasional transaction in cash amounting to a value of at least EUR 3 000** (…). 5) (…) providers of gambling services shall **apply customer due diligence** measures (…) when carrying **out transactions amounting to at least EUR 2 000** (…)	
Customer due diligence measures Article 20	Customer due diligence is a **multi-step, risk-based process** that goes beyond simple identification. Gatekeepers must build a holistic profile to identify who truly benefits from the relationship and evaluate if the client's profile **matches their actual activities**. This ensures the obliged entity is not merely checking boxes but **actively assessing the likelihood** of the relationship being misused for criminal ends.
1) For the purpose of conducting customer due diligence, **obliged entities shall apply all of the following measures**: (a) **identifying the customer** and verifying the beneficial owners and taking reasonable measures to verify their identity (…) (c) assessing and (…) **understanding the purpose and intended nature of the business relationship** (…) (f) **conducting ongoing monitoring of the business relationship** (…)	

Inability to comply with the requirement to apply customer due diligence measures Article 21	
1) **Where an obliged entity is unable to comply with the requirement** to apply customer due diligence measures (…) **it shall refrain from carrying out a transaction** or establishing a business relationship and shall terminate the business relationship and consider reporting a suspicious transaction to the FIU (…).	**If an obliged entity is unable to complete identity checks** because the clients are evasive or documents are missing, it is legally forbidden from providing services. **The relationship must be ended**, and the entity must evaluate if the situation is suspicious.
Identification and verification of the identity of customers and beneficial owners Article 22	
1) (…) **obliged entities shall obtain** at least the following **information** (…) (a) for a natural person: (i) all names and surnames; (ii) place and full date of birth; (iii) nationalities (…) (iv) place of residence (…) for a legal entity: (i) legal form and name (ii) address of the registered or official office (iii) name of the legal representatives (…) 2) – 5) (…) 6) Obliged entities shall obtain the information, documents and data necessary for the verification of the identity of the customers and of any person purporting to act on their behalf	**Obliged entities must collect a specific set of verified personal or corporate data** using official independent sources like passports or government-approved electronic IDs.

Timing of the verification of the customer and beneficial owner identity Article 23	
4) **Whenever entering into a new business** relationship with a legal entity or the trustee of an express trust or the person holding an equivalent position **(…) obliged entities shall collect valid proof of registration** or a recently issued excerpt of the register confirming validity of registration.	The 'check before acting' rule serves as the primary gateway to the financial system, **preventing illicit funds from ever entering.** The law allows a **pragmatic balance for low-risk scenarios** where business must move quickly, provided that the identity check is finalised immediately after and the delay does not create a vulnerability that criminals could exploit.
Reporting of discrepancies with information contained in beneficial ownership registers Article 24	
1) **Obliged entities shall report to the central registers any discrepancies they find between the information available in the central registers and the information they collect** (…), obliged entities shall accompany their reports with information they have obtained (…). 2) (…) obliged entities may (…) **request additional information** from the customers where the discrepancies identified: (b)are a result of outdated data, but the beneficial owners are known to the obliged entity. When an **obliged entity concludes that the beneficial ownership information in the central register is incorrect**, it shall **invite the customer to submit the correct information** to the central register. 3) **Where a customer has not submitted the correct information within the deadline** (…) the **obliged entities** shall **report the discrepancy** to the central register. (...) The requirement of this Article shall apply when the obliged entities (…) provide legal advice in any of the situations.	**Obliged entities act as secondary verification layer for information held in public records**. If they find that the government's official database of company owners is incorrect compared to their own research, they must report the error within two weeks. This **helps ensure public registries stay accurate** though minor typos or known outdated info can be resolved with the client first.

Identification of the purpose and intended nature of a business relationship or occasional transaction Article 25	
Before entering into a business relationship or performing an occasional transaction, an obliged entity shall assure itself that it understands its purpose and intended nature. To that end, the obliged entity shall obtain (…) information.	**Understanding the 'why' and 'how' of a relationship** is essential to establishing a **baseline of normal behaviour**. By verifying the economic logic and the origin of wealth, gatekeepers can effectively **distinguish between legitimate commercial activity and unusual patterns** that may indicate an attempt to hide proceeds of crime.
Ongoing monitoring of the business relationship and monitoring of transactions performed by customers Article 26	
1) Obliged entities shall conduct ongoing monitoring of business relationships (…) throughout the course of a business relationship (…) ensure that those transactions are consistent with the obliged entity's knowledge of the customer (…) and to detect those transactions that shall be made subject to a more thorough assessment (…). 2) (…) Obliged entities shall ensure that the relevant documents, data or information of the customer are kept up to date. (…) 3) (…) obliged entities shall review (…), and update the customer information where: (…) (b) the obliged entity has a legal obligation in the course of the relevant calendar year to contact the customer (…) 4) In addition (…) obliged entities shall regularly verify whether the conditions (..) are met. The frequency of that verification shall be commensurate with the exposure of the obliged entity and the business relationship to risks oof non-implementation and evasion of targeted financial sanctions.	**Because risk is dynamic, not static**, gatekeepers must **continuously watch for shifts in behaviour** that no longer match the client's original profile. Mandatory updates (e.g.; annually for high-risk clients) ensure that the **entity's risk assessment remains current** and that **new, suspicious patterns are detected** before they can mature into large-scale laundering operations.

Regulatory technical standards on the information necessary for the performance of customer due diligence Article 28	
1) **AMLA shall develop draft regulatory technical standards** (…) [that] specify: (a) the **requirements** (…) and the **information** to be **collected** for the purpose of performing standards, simplified and enhanced due diligence (…) (d) the **reliable and independent sources of information** that may be used to verify the identification data (…) 2) (…) 3) AMLA shall review regularly the regulatory technical standards and, if necessary, prepare and submit to the Commission (…)	**By standardising exactly which documents are valid and what data points are required**, these standards **provide legal certainty** for businesses and ensure that criminals cannot shop for jurisdictions with lower verifications standards.

Third-country policy and money laundering and terrorist financing threats from outside the Union
Section 2 – Chapter III

Article 29

1**) Third countries with significant strategic deficiencies** in their national AML/CFT regimes shall identified by the Commission and **designated as 'high-risk third countries'** (…)

4) (…) obliged entities shall apply enhanced due diligence measures (…) with respect to the business relationships or occasional transactions involving natural or legal from that third country.

5) The delegated act (…) **shall identify among the countermeasures listed in Article 35 the specific countermeasures** mitigating specific risks stemming from each high-risk third country

Article 30

1) Third countries with compliance weaknesses in their national AML/CFT regimes shall be identified by the Commission. (…)

4) The delegated act (…) shall **identify the specific enhanced due diligence measures (…) the obliged entities shall apply to mitigate risks** related to business relationships or occasional transactions involving natural or legal person from that third country.

These Articles categorise external threats into three levels:

- **High-risk countries** with persistent structural failures
- **Countries with specific compliance weaknesses**
- **Countries posing sudden, exceptional threats that fall outside standard categories.**

For gatekeepers, these designations are not just informational; **they trigger mandatory legal obligations**.

Depending on the severity of the threat, professional entities must apply **rigorous Enhanced Due Diligence** (e.g.: deeper wealth tracing) or follow strict countermeasures that may limit or even block certain transactions. This coordinated response ensures that **legal or institutional failures in foreign jurisdictions do not contaminate the Union's financial system or undermine its security.**

NB: Article 35 on third-country policy on money-laundering and terrorist financing threats from the Union.

Article 31 1) The Commission is empowered to adopt delegated acts (…) by **identifying third countries where in exceptional cases it considers it indispensable to mitigate a specific and serious threat to the Union's financial system** (…) and which cannot be mitigated pursuant to Article 29 and 30. 6) Where the identified (…) threat (…) amounts to a significant strategic deficiency, Article 29 (4) shall apply and the delegated act (…) shall specify specific countermeasures 7) **Where the identified (…) threat (…) amounts to a compliance weakness, the delegated act (…) shall identify specific enhanced due diligence measures.**	
Guidelines on money laundering and terrorist financing risks, trends and methods Article 32	
1) (...) **AMLA shall issue guidelines** defining the **money laundering and terrorist financing risks, trends and methods** involving any geographical area outside the Union to which obliged entities are exposed (…) Where situations of higher risk are identified, the guidelines shall include **enhanced due diligence measures that obliged entities shall consider applying to mitigate such risks**.	To ensure gatekeepers remain resilient against evolving global threats, a central authority provides **regular updates on emerging criminal patterns** and geographic vulnerabilities. Obliged entities must use these insights to **adapt their internal controls** and apply enhance due diligence when dealing with regions identified as having elevated risk levels.

Simplified due diligence
Section 3 – Chapter III

Article 33

1) Where (…) the business relationship or transaction present a **low degree of risk, obliged entities may apply (…) simplified due diligence measures:**

(b) reducing the frequency of customer identification updates;

(c) reducing the amount of information collected (…)

Article 34

1) (…) **obliged entities shall apply enhanced due diligence measures to manage and mitigate [higher] risks** appropriately (…)

2) Obliged entities shall **examine the origin and destination** of funds (…) that fulfil at least one of the following conditions:

(a) the transaction is of a complex nature;

(b) the transaction is unusually large;

(c) the transaction is conducted In an unusual pattern;

(d) the transaction does not have an apparent economic or lawful purpose;

4) (…) Obliged entities shall **apply enhanced due diligence** measures, **proportionate to the higher risks identified**, which may include the following measures:

(a) obtaining additional information on the customer and the beneficial owners;

(c) (…) information of funds, and source of wealth of the customer and of the beneficial owners;

(e) obtaining the approval of senior management for establishing or continuing the business relationship

When risks are high, due to complex deals, massive sums, or suspicious patterns, obliged entities must conduct deeper scrutiny of the client's total wealth and the specific origin of their money, ensuring that high-level management takes accountability for the relationship.

Article 41- 42	
Article 41 (…) With respect to customers who are **third-country nationals who are in the process of applying for residence rights** in a Member State in exchange **for any kind of investment** (…) obliged entities shall, as a minimum, **apply enhanced due diligence** measures set out in Article 34(4) (…). **Article 42** 1) (…) Obliged entities shall apply the following measures with respect **to (…) politically exposed persons**: (a) obtain senior management approval (…) (b) take adequate measures to establish the source of wealth and source of funds (…) (c) **conduct enhanced, ongoing monitoring of those business relationships.**	Certain clients are classified as high-risk by nature because their status or the services they seek (such as golden visas or prominent public office) are highly vulnerable to corruption. For these individuals, gatekeepers are legally required to use the strictest level of scrutiny. This includes full transparency regarding the origin their entire fortune, subjecting the relationship to continuous monitoring, and ensuring that senior management personally approves and oversees the engagement to prevent abuses of public power or financial loopholes.

Politically exposed persons who are beneficiaries of insurance policies Article 44	
(…) Obliged entities shall take reasonable measures to determine whether the beneficiaries of a life or other investment-related insurance policy (…) are **politically exposed persons**. That measure shall be taken no later at the time of the payout or at the time of the assignment (…) Where there are higher risks identified (…) obliged entities shall: (a) **inform senior management before payout** of policy proceeds (b) **conduct enhanced scrutiny of the entire business relationship** with the policyholder	High-risk individuals like politically exposed persons can use insurance payouts to launder money. Gatekeepers must check beneficiaries before any money is paid out. If a politically exposed person is identified, the law requires high-level management to approve the payment and a deeper investigation into the client who bought the policy to ensure the funds aren't linked to corruption.
Measures for persons who cease to be politically exposed persons Article 45	
1) Where a politically exposed person is **no longer entrusted with a prominent public function** (…) obliged entities shall **take into account the continuing risk posed by that person**, as a result of his or her former function (…) 2) Obliged entities **shall apply one or more of the [enhanced] measures (…) for not les than 12 months** following the time when the individual ceased to be entrusted with a prominent public function.	A person doesn't stop being a risk the day they leave office; they may still hold significant informal influence or have active criminal connections. Therefore, entities must continue to apply extra scrutiny for at least one year after the client leaves their public role, or longer if the specific risk of the former function remains

Reliance on customer due diligence performed by other obliged entities
Section 6 – Chapter III

Article 48

1) **Obliged entities may rely on other obliged entities (…) to meet the customer due diligence requirements (…)** provided that:

(a) the other obliged entities apply due diligence requirements and record-keeping laid down in this Regulation, or equivalent (…)

(b) compliance with AML/CFT (…) is **supervised** in a manner consistent with Chapter IV of Directive (EU) 2024/1640.

The ultimate responsibility (…) shall remain with the obliged entity which relies on another obliged entity.

Article 49

1**) Obliged entities shall obtain from the obliged entity relied upon all the necessary information** (…)

2) Obliged entities (…) shall take the necessary steps to ensure that the obliged entity relied upon provides upon request:

(a) copies of the information collected to identify the customer

(b) all supporting documents (…)

3) The information (…) shall be provided (…) **without delay and in any case within 5 working days.**

4) The conditions for the transmission (…) shall be specified in a **written agreement.**

To prevent repetitive paperwork and improve efficiency, businesses can **use identity checks already performed by others.** However, the business making the choice is still **legally responsible for any failures**. They must have a formal written agreement, be able to get all underlying **documents immediately (within 5 days**), and ensure the other party is properly supervised. This balanced approach allows for economies of scale while maintaining strict security standards.

Article 50 By 10 July 2027, **AMLA shall issue guidelines** addressed to obliged entities on: (a) the **conditions which are acceptable for obliged entities to rely on information** (…) (b) the roles and responsibility of the obliged entities (…) (c) supervisory approaches to reliance on other obliged entities	
Reporting of suspicions Article 69	
1) Obliged entities (…) shall cooperate fully with the FIU by promptly: (a) reporting to the FIU, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds or activities (…) are the proceeds of criminal activity or are related to terrorist financing (…). 5) (…) **AMLA shall issue guidelines on indicators of suspicious activity** or behaviours. 6) The **compliance officer (…) shall transmit the information** (…) to the FIU of the Member State in whose territory the obliged entity (…) is established. 7) Obliged entities shall ensure that [staff] involved in the performance of the tasks covered by this Article are **protected against retaliation, discrimination and any other unfair treatment**.	The detection of financial crime relies on the '**gatekeeper' role** of professional entities, which must act as an **early warning system** by reporting any suspicion of illicit activity to the FIU. Detection must be based on a **holistic assessment of patterns and behaviour**, supported by Union-wide indicators, rather than just fixed transaction amounts. Critically, the law provides **mandatory protection for employees**, ensuring they can fulfil their **reporting duties without fear** of professional or personal consequences

Specific provisions for reporting of suspicions by certain categories of obliged entities Article 70	
1) (...) Member States may allow **obliged entities [such as lawyers] to transmit the information (...) to a self-regulatory body** designated by the Member State. 2) Notaries, lawyers, other independent legal professionals, auditors, external accountants and tax advisors shall be exempted (...) to the extent that such exemption relates to information that they receive from, or obtain on a client, in the course of ascertaining the legal position of that client, or performing their task of defending or representing that client in (...) judicial proceedings (...) **The exemption (…) shall not apply when [they]:** **(a) take part in money laundering (...)** (b) **provide legal advice for the purposes of money laundering** (...) or (c) know that the **client is seeking legal advice for the purposes of money laundering.**	**This article balances the fight against crime with the fundamental right to professional secrecy and legal defence**. Information obtained while defending a client or providing a legal opinion is generally protected to ensure the right to a fair trial. However, this protection is not absolute; it is automatically waived if the professional participates in the crime or if the legal advice is being used to facilitate money laundering. In such cases, the duty to protect the integrity of the financial system overrides the duty of confidentiality
Refraining from carrying out transactions Article 71	
1) **Obliged entities shall refrain from carrying out transactions** which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have submitted a report (...) and have complied with any further specific instructions from the FIU (...). Obliged entities may carry out the transaction (...) if they have **not received instructions to the contrary from the FIU within 3 working days** of submitting the report. 2) Where it is **not possible (...) to refrain (...) or where refraining would be likely to frustrate efforts** to pursue the beneficiaries (...) the obliged entity shall **inform the FIU immediately after** carrying out the transaction.	Gatekeepers must **halt suspicious transactions** immediately to allow authorities time to intervene. This **mandatory cooling-off period** ensures that suspected illicit funds are not moved before the FIU can act. However, if stopping the transaction is physically impossible or would **alert the criminals** (tipping them off) and sabotage an investigation, the entity may proceed but must **notify the FIU immediately afterward**.

Prohibition of disclosure Article 73	
1) **Obliged entities and their directors, employees (...) shall not disclose to the customer concerned or to other third persons** the fact that transactions or activities are being or have been assessed (...) or that a money laundering or terrorist financing analysis is being, or may be, carried out. (...) 3) (...) **disclosure may take place between obliged entities that belong to the same group** (...) 5) (...) in cases relating to the **same transaction involving two or more obliged entities** (...) disclosure may take place between [them] provided they are **located in the Union** (...) and that they are subject to professional secrecy.	The article prohibits "tipping off": obliged entities and their staff cannot reveal that a customer is being assessed for potential money laundering. Limited information-sharing is allowed only within the same group or between EU-based entities involved in the same transaction, provided all parties are bound by professional secrecy.
Exchange of information in the framework of partnerships for information sharing Article 75	
1) Members of **partnerships for information sharing may share information** among each other where **strictly necessary** for the purposes of complying with [due diligence and reporting] obligations (...). 3) Information exchanged (...) shall be **limited to:** **(a) information on the customer (...)** **(c) information on customer transactions (...)** **(g) information on suspicions** (...). 4) (...) (b) obliged entities **shall not rely solely on the information received** (...) to comply with the requirements (...) (c) obliged entities **shall not draw conclusions or take decisions** (...) without having assessed that information.	Entities can join formal **collaborative platforms** to share data on high-risk clients and suspicious patterns, which enhances the collective ability to spot complex crime. However, this is **strictly regulated** to protect privacy; participation requires **prior notification to supervisors**. Importantly, a gatekeeper **cannot outsource its judgment**; it must still perform its own independent assessment and cannot automatically reject a client based solely on data from a partner.

Record retention Article 77	
1) **Obliged entities shall retain** the following documents (...): (a) a **copy of the documents and information obtained in the performance of customer due diligence** (...) (c) the **supporting evidence and records of transactions** (...) necessary to identify transactions. 3) The information (...) shall be **retained for a period of 5 years** commencing on the date of the **termination of the business relationship** or on the date of the **carrying out of the occasional transaction**. (...) obliged entities shall **delete personal data upon expiry of the five-year period**.	Entities must keep all identity documents and transaction records for a **uniform period of 5 years** after the relationship ends. To balance security with **privacy rights**, the law also mandates the **automatic deletion** of this personal data once the 5-year window closes, unless authorities specifically request an extension for an ongoing investigation
Provision of records to competent authorities Article 78	
Obliged entities shall have systems in place that enable them to respond fully and speedily to enquiries from their FIU or from other competent authorities (...) as to whether they are maintaining or have maintained, during a **five-year period prior to that enquiry a business relationship with specified persons**, and on the nature of that relationship. (…)	The article requires obliged entities to maintain systems that allow them to quickly disclose to authorities whether they have a business relation with a specific person. This requires having **efficient retrieval systems** that allow for a rapid response to official inquiries. The goal is to ensure that law enforcement can **trace assets in real-time** across the financial system, requiring entities to confirm quickly if a suspect has held an account or conducted business with them.

DIRECTIVE 2024/1640 – AMLD6

RELEVANT LEGISLATION

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31st May 2024 on the mechanisms to be put in place by MS for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU)2019/1937, and amending and repealing Directive (EU) 2015/849 (known as the AMLD6)

PROVISIONS	EXPLAINER
Subject matter, scope and definitions Section 1	
Article 1 This Directive lays down rules concerning: (b) the requirements in relation to registration of, identification of, and checks on, senior management and beneficial owners of obliged entities; (f) the responsibilities and tasks of bodies involved in the supervision of obliged entities **Article 2** The following definitions also apply: (4) 'obliged entities' means a natural or legal person listed in Article 3 of Regulation (EU) 2024/1624 that is not exempted in accordance with Article 4, 5, 6 or 7 of that Regulation; (6) **'host Member State' means a Member State, other than the home Member State, in which the obliged entity operates an establishment,** (…), or where the obliged entity operates under the freedom to provide services through an infrastructure	//

Identification of exposed sectors at national level Article 3	
1) Where a Member State identifies that, in addition to obliged entities, entities in other sector are exposed to money laundering and terrorist financing risks, it may decide to apply all or part of Regulation (EU) 2024/1624 to those additional entities.	//
Requirements relating to certain service providers Article 4	
1) Member States shall ensure that **currency exchange and cheque cashing offices, and trust or company service providers, are either licensed or registered**. (…) 2) (…) 3) Member States shall ensure that **obliged entities** other than those referred to in paragraphs 1 and 2 **are subject to minimum registration requirements** which enable supervisors to identify them. (…)	To provide effective oversight, **authorities must be able to identify every entity operating in a protected sector**. While some high-risk businesses require a formal licence to operate, even those in less regulated professions must at least be registered so that supervisors can keep track of their activity and ensure they are fulfilling their duties.

Checks on the senior management and beneficial owners of certain obliged entities Article 6	Since these entities hold a position of trust, AMLD6 requires that the **people who run or own them are honest and qualified.** If a manager is found to have a criminal record, the authorities have the power to force their removal or ban them from the industry.
1) **Member States shall require supervisors** to verify that the members of **the senior management in the obliged entities** (…) and the beneficial owners of such entities are of **good repute, and act with honesty and integrity**. Senior management of such entities shall also **possess the knowledge and expertise necessary to carry out their functions**. (…) 4) Member States shall ensure that **supervisors have the power to request the removal of any person convicted of money laundering** (…) from the senior management of obliged entities (…)	**AMLD5 vs AMLD6** AMLD6 moves beyond the general prudential suggestions of AMLD5 by codifying rigorous 'fit and proper' checks. Supervisors must verify the honesty and integrity of senior management and beneficial owners and are granted the explicit power to remove or temporarily ban individuals convicted of relevant crimes from an obliged entity.
National risk assessment Article 8	Member States conducts broad assessments of national risks and is required to share these findings with the private sector. This helps the entities tailor their own internal checks to focus on the specific areas where the danger of illicit activity is highest.
4) **Member States shall use the national risk assessment to**: (a) **improve their AML/CFT regimes**, in particular any areas where obliged entities are to apply enhanced measures in line with a risk-based approach (…); (f) **make appropriate information available promptly to competent authorities and to obliged entities** to facilitate the carrying out of their own money laundering and terrorist financing risk assessments (…)	**AMLD5 vs AMLD6** Evolving from the resource-reporting focus of AMLD5, AMLD6 transforms the risk assessment into a strategic tool. Member States must now evaluate the evasion of targeted financial sanctions and share findings with obliged entities to facilitate their own risk assessments.

Central beneficial ownership registers
Article 10

1) **Member States shall ensure that beneficial ownership information** (…) and information on nominee arrangements (…) **are held in a central register in the Member States** (…)

5) (b) (…) Member State shall ensure that **[this] information (…) is available to competent authorities**, as well as to **AMLA** for the purposes of joint analyses, (…) to self-regulatory bodies and to obliged entities**. However, obliged entities shall only have access to the statement submitted by the legal entity** or legal arrangement if they report a discrepancy (…) or provide proof of the steps they have taken to determine the beneficial owners of the legal entity or legal arrangement, in which case they shall be able to access the justification as well.

7) (b) (…) **the Commission shall issue recommendations on the methods and procedures to be used by entities in charge of central registers to verify beneficial ownership information** and by obliged entities and competent authorities to identify and report discrepancies regarding beneficial ownership information.

When obliged entities act as trustees, they are responsible for the accuracy of the data they submit to central registries. **To ensure they are not hiding the true owners of assets, authorities can conduct physical inspections of their offices**. If they provide false or outdates information, they can face significant fines or other legal penalties.

AMLD5 vs AMLD6

AMLD6 significantly bolsters the verification powers of the authorities managing central registers. They are now empowered to conduct physical on-site inspections at the business premises of obliged entities acting as trustees and must perform **immediate automated screening against targeted financial sanctions lists.**

General rules regarding access to beneficial ownership registers by competent authorities, self-regulatory bodies and obliged entities Article 11	
3) Member States shall ensure that, **when taking customer due diligence measures (…) obliged entities have timely access to the information held in the interconnected central registers** (…) 4) **Member States may choose to make beneficial ownership information (…) available to obliged entities upon payment of a fee,** which shall be limited to what is strictly necessary to cover the costs (…) 5) (…) **Member States shall notify to the Commission the list of** competent authorities and self-regulatory bodies and the categories of **obliged entities that were granted access to the central register and the type of information** available to obliged entities.	To properly verify who their customers are, these entities must have access to official government records. This Article guarantees them this access so they can perform their backgrounds checks effectively. While a fee may be charged, it must be kept low, so it does not discourage them from using the data. NB: Article 15 on the exceptions to the access rules to beneficial ownership registers.
Establishment of the FIUs Article 19	
2) **The FIU shall** be the single central national unit responsible for receiving and **analysing reports submitted by obliged entities** (…) 3) (…) it shall be able to obtain additional information from obliged entities.	The Financial Intelligence Unit (FIUs) acts as the central hub for reports on suspicious activity. **The obliged entities are required to send their suspicions on fraudulent transactions to the FIUs for analysis**. Furthermore, FIUs has legal authority to contact an entity and demand further details about a customer or transaction to help build a criminal case.

Alerts to obliged entities Article 26	To help obliged entities protect themselves, FIUs must warn them about known threats. This includes **flagging dangerous regions, suspicious individuals, or new criminal methods.** By providing this 'strategic intelligence', the FIU enables businesses to **fine-tune their internal risk checks**, ensuring they are looking for the right red flags and effectively acting as gatekeepers against illicit finance.
1) Member States shall ensure that FIUs are able to **alert obliged entities of information relevant for the performance of customer due diligence** (…). That information shall include: (a) **types of transactions or activities** that present a significant risk (…); (b) **specific persons** that present a significant risk (…); (c) **specific geographic** areas that present a significant risk (…) 3) FIUs shall provide obliged entities **with strategic information about typologies, risk indicators and trends** (….) on annual basis.	**AMLD5 vs AMLD6** There is a shift from passive feedback of AMLD5 under AMLD6. The FIU is now mandated to issue strategic alters directly to obliged entities regarding specific persons, transactions, or geographic areas that present
Feedback by FIU Article 28	
1) Member States shall ensure **that FIUs provide obliged entities with feedback on the reporting of suspicions** (…). Such feedback shall **cover at least the quality of the information provided, the timeliness of reporting, the description of the suspicion and the documentation** provided (…) The FIU shall provide feedback at least **once per year** (…)	//

Powers and resources of national supervisors
Article 37

1) Each Member State shall ensure that obliged entities established in its territory (…) are subject to adequate and effective supervision (…)

5) (…) national supervisors perform the following tasks:

(a) to disseminate relevant information to obliged entities (…)

(c) to verify the adequacy and implementation of the internal policies, procedures and controls (…);

(f) to conduct all the necessary off-site investigations, on-site inspections and thematic checks (…)

6) (…) supervisors have (…) the power to:

(a) compel the production of any information from obliged entities which is relevant for monitoring and verifying compliance (…).

Supervisors are not just passive observers; they must **actively inspect business premises, review internal files**, and **demand any document** they need to verify that a business is following the rules. This ensure that every entity, regardless of its size, is effectively managing its risks and maintaining the integrity of the financial system.

AMLD5 vs AMLD6

AMLD6 gives supervisors a more intrusive toolkit than the adequate powers in AMLD5. Supervisors are now empowered to inspect premises without prior announcement and **have direct right to access an obliged entity's internal software, databases, and IT tools.**

Supervision of forms of infrastructure of certain intermediaries operating under the freedom to provide services
Article 38

Where the activities of the following obliged entities are carried out in their territory under the freedom to provide services through agents or distributors, or through other types of infrastructure (…) Member States shall ensure that such activities are subject to supervision by their national supervisors:

(a) electronic money issuers (…)

(b) payment service providers (…); and

(c) crypto-asset service providers.

To prevent gaps in oversight, the **host Member State takes responsibility for supervising** these specific providers. This ensures that even without a local head office, the way **they interact with the local market is monitored to prevent criminal abuse** of their services.

Provision of information to obliged entities Article 39	
1) Member States shall ensure that **supervisors make information on money laundering and terrorist financing available to the obliged entities** under their supervision (…) 3) Member States shall ensure that supervisors **carry out outreach activities**, as appropriate, **to inform the obliged entities** under their supervision of their obligations. 4) Member States shall ensure that supervisors **make information on persons or entities designated in relation to targeted financial sanctions and UN financial sanctions available to the obliged entities** under their supervision immediately.	To act as effective gatekeepers, obliged entities need up-to-date intelligence from the Member States. Supervisors are required to share **risk assessments, guidance on criminal methods, and immediate alerts** about sanctioned individuals. This proactive sharing of information empowers entities to **properly classify their customers** and recognize the red flags that indicate a high risk of illicit activity.
Risk-based supervision Article 40	
1) Member States shall ensure that **supervisors a risk-based approach to supervision**. (…) 2) (…) **AMLA shall develop draft regulatory technical standards** (…) [which] set out the benchmarks and a methodology for assessing and classifying the inherent and residual risk profile of obliged entities (…) 4) Member States shall ensure that supervisors **take into account the degree of discretion allowed to the obliged entity and appropriately review the risk assessment** underlying this discretion, and the adequacy of its internal policies, procedures and controls.	Supervisors must assess the inherent **risk profile of each obliged entity** and adjust the intensity of their inspections accordingly. By **reviewing how an obliged entity exercises its own judgment** in assessing risks, authorities can verify that the business's **internal defences are strong enough** to withstand criminal attempts.

Articles 45-47	
Article 45 1) Member States shall ensure that the **supervisors of the home Member State** inform the supervisors of the host Member State as soon as possible (…) of the **activities that the obliged entity intends to carry out** in the host Member State. **Article 46** 1) **In the case of credit institutions and financial institutions** that are part of a group, (…) **financial supervisors of the home Member State and those of the host Member State cooperate with each other to the greatest extent possible**. 6) Member States shall ensure that this Article also applies to the supervision of: (…) (b) **obliged entities operating under the freedom to provide services without any infrastructure in another Member States than the Member States where they are established**. (…) Member States shall also ensure that **in cases where obliged entities in the non-financial sector are part of structures** which share common ownership, management or compliance control, including networks or partnerships, non-financial supervisors cooperate and exchange information. **Article 47** 1) Where **obliged entities that are not part of a group carry out cross-border activities** (…) and **supervision is shared** (…) Member States shall ensure that those **supervisors cooperate with each other to the greatest extent possible.**	When obliged entities operate across multiple Member States, supervisors must work as a team to prevent criminal from exploiting national borders. This involves **sharing information about a company's structure, its beneficial owners, and its internal controls**. By communicating constantly, authorities can ensure that a **group's global policies are being applied effectively** in every local office, preventing weak links in the chain.

Articles 49-50

Article 49

1) Member States shall ensure that **dedicated AML/CFT supervisory colleges are set up** (…) where a credit institution or financial institution (…)

(b) has set up establishments in at least two different Member States (…)

14) (…) **draft regulatory technical standards shall specify**: (…)

(c) any **additional measure to be implemented by the colleges when groups include obliged entities in the non-financial sector**

Article 50

1) Member States shall ensure that the non-financial supervisors (…) are able to set up dedicated AML/CFT supervisory colleges (…)

(a) where an obliged entity in the non-financial sector, or a group thereof, has set establishments in at least two different Member States (…)

Permanent structures for cooperation, known as colleges, **are established for large organisations operating across border**. These colleges allow supervisors from different Member States **to coordinate their oversight and exchange intelligence**. Whether the business is a bank or a non-financial entity like a law firm group, these colleges **ensure a unified supervisory approach,** allowing authorities to address serious breaches that affect the entire group simultaneously.

AMLD5 vs AMLD6

There is a shift from the voluntary and guideline-based cooperation seen under AMLD5 to a mandatory legal requirement in AMLD6. Member States must now establish a joint supervisory framework for any obliged entity -financial or non-financial- that operates across multiple Member States. For the obliged, this means facing a unified and permanent supervisory front where supervisors from different jurisdictions coordinate their approach to inspections and the imposition of measures for serious breaches.

Oversight of self-regulatory bodies Article 52	
1) Where Member States decide (…) to **allow self-regulatory bodies to perform supervision of the obliged entities** (…) they shall ensure that the activities of such self-regulatory bodies in the performance of such functions are **subject to oversight by a public authority.** 2) The public authority-overseeing self-regulatory bodies shall be responsible for **ensuring an adequate and effective supervisory system for the obliged entities** (…)	In sectors where professional bodies manage the oversight of an obliged entity, the Member State must **appoint a public authority to monitor those bodies**. This ensures that **the obliged entity is held to a high standard of compliance and that the supervisory system is free from industry influence**, maintaining the integrity of the internal market.
General provisions Article 53	
1) Member States shall ensure that obliged entities can be held liable for breaches of Regulation (EU) 2024/1624 and (EU) 2023/1113 in accordance with this Section.	//
Supervisory measures towards establishments of obliged entities and certain activities carried out under the freedom to provide services Article 54	
2) Where the **supervisors** of the host Member State identify breaches (…) they **shall request the obliged entities** operating through the establishments (…) to **comply with the applicable requirements** (…) 3) Where the obliged entities fail to take necessary actions, the **supervisors of the host Member State shall inform the supervisors of the home Member State** accordingly. 4) (…) in situation of serious, repeated or systematic breaches by obliged entities (…) supervisors of the host Member State shall be allowed at their own initiative to take appropriate and proportionate measures (…).	When an obliged entity operates across borders, **the host Member State has the authority to demand they fix any identified breaches**. If the **failures** of the obliged entity **are severe or persistent**, the local supervisor can take **immediate temporary action to protect their territory's** financial system until the home Member State can intervene.

Pecuniary sanctions Article 55	
1) **Member States shall ensure that pecuniary sanctions are imposed on obliged entities for serious, repeated or systematic breaches** (…) of the requirements laid down in (…): (a) Chapter II (Internal policies, procedures and controls of obliged entities) (b) Chapter III (Customer due diligence) (c) Chapter V (reporting obligations) (…) 2) (…) the maximum pecuniary sanctions (…) amount at least to twice the amount of the benefit derived from the breach (…) or at least EUR 1 000 000, whichever is higher.	Member States must **impose significant fines on an obliged entity for major failures** in core duties like checking customers or reporting suspicions. By setting a high financial floor for these penalties, the Article ensures that obliged entity views AML/CFT compliance as a critical legal necessity rather than just an administrative cost.
Administrative measures Article 56	
1) **Member States shall ensure that supervisors are able to apply administrative measures to an obliged entity** where they identify: (a) **breaches** (…) (b) weakness in the internal policies (…) 2) Member States shall ensure that **supervisors are able** at least to: (…) (b) **order obliged entities to comply**, including to implement specific corrective measures (e) **impose a temporary ban against any person discharging managerial responsibilities in an obliged entity**, or any other natural person who has been held responsible for the breach from exercising managerial functions in obliged entities	Beyond fines, **supervisors need effective tools to compel an obliged entity to change its behaviour**. These enforcement measures, such as **public statements that expose compliance failures the entity** or **the withdrawal of the license**, are designed by the Member State to correct internal deficiencies and ensure the obliged entity operates safely and legally.

Periodic penalty payments Article 57	If an obliged entity fails to comply with an order to improve its compliance systems, the Member State can apply constant financial pressure via **daily fines**. This serves to **force immediate compliance**, making it clear to the **obliged entity** that stalling on legal requirements will result in escalating costs.
1) **Member States shall ensure that, where obliged entities fail to comply with administrative measures** (…) within the applicable deadlines, supervisors are able to **impose periodic penalty payments in order to compel compliance** with those administrative measures 2) (…) The periodic penalty payments shall be imposed until the obliged entity or person concerned complies with the relevant administrative measures.	**AMLD5 vs AMLD6** This is a new enforcement mechanism under AMLD6 that was not detailed in AMLD5. Member States must now empower supervisors to impose daily fines to compel an obliged entity to comply with a previous administrative order. This ensures that an obliged entity cannot simply delay compliance, as the financial cost of inaction increases every single day.
Reporting of breaches and protection of reporting persons Article 60	**Member States must guarantee the safety of "whistleblowers" within an obliged entity**. By setting up secure channels for employees to report violations, the Member State ensures that internal failures or criminal acts within an obliged entity can be brought to light without the reporting person fearing retaliation.
1) (...) reporting of breaches (...) and to the **protection of persons reporting such breaches** (...) 2) **Supervisory authorities** shall be the authorities competent to establish **external reporting channels** and to follow-up on reports insofar as requirements applicable to **obliged entities** are concerned (...)	

AML/CFT cooperation Section 1 – Chapter V	
Article 61 3) **Member States shall not prohibit or place unreasonable or (...) restrictive conditions on the exchange of information** (...) do not refuse a request for assistance on the grounds that: (...) (b) national law requires **obliged entities to maintain secrecy or confidentiality** (...). **Article 62** 1) (...) **Member States shall communicate to the Commission and AMLA:** **(a) the list of supervisors** responsible for overseeing the compliance of the **obliged entities** (...) and their contact details; (...).	Effective cooperation requires that Member States do not allow national laws, such as professional secrecy of an obliged entity, to block the exchange of intelligence information between authorities. Furthermore, by **keeping a centralized list of all supervisors, the Union ensures that every obliged entity is properly monitored** and that cross-border assistance is fast and efficient.
Professional secrecy requirements Article 67	
1) **Member States shall require that all persons working for (...) supervisors (...) [to] be bound by the obligation of professional secrecy**. (...) confidential information (...) receive in the course of their duties (...) may be **disclosed only in summary or aggregate form, in such a way that individual obliged entities cannot be identified.**	While supervisors have broad powers, the Member State must also protect the legitimate business secrets of an obliged entity. Any sensitive data received during an investigation must remain confidential. If the supervisor shares data, they must do so in a way that **prevents the identification of the entity involved**. This confidentiality requirements helps maintain trust in the supervisory system.

AML/CFT cooperation guidelines
Article 69

By 10 July 2029, AMLA shall (...) issue guidelines on:

(a) the cooperation between competent authorities (...) and the entities in charge of the central registers, to prevent money laundering and terrorist financing;

(b) the **procedures to be used by authorities competent for the supervision or oversight of obliged entities under other Union legal acts** (...).

To ensure a unified defence, AMLA provides instructions on how all authorities within a Member State should work together. This framework ensures that even those overseeing an obliged entity for other purposes – such as banking stability-understand how to **identify and address money laundering risks** within that specific obliged entity. By aligning their roles and information flows, the system delivers a unified and consistent defence across all supervisory fronts.

AMLD5 vs AMLD6

Evolving from the sectoral guidance of AMLD5, AMLD6 centralises the creation of cooperation standards under AMLA. These now mandatory guidelines will define how supervisors must take money laundering risks into account when performing other duties (such as prudential banking checks). For the obliged entity, this creates a more unified supervisory experience where AMLD/CFT expectations are integrated across all forms of state oversight, rather than treated as separate compliance track

REGULATION 2024/1620 – AMLA REGULATION

RELEVANT LEGISLATION

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulation (EU) No 1094/2010 and (EU) No 1095/2010 (known as the AMLA Regulation)

PROVISIONS	EXPLAINER
Definitions Article 2	AMLA Regulation establishes a distinction between the types of companies subject to oversight. **This differentiation allows the Union to concentrate its direct resources on those institutions that present the highest cross-border risk**, while ensuring that all other entities remain subject to a common, high-quality standard enforced at the national level.
1) (…) (1) **'Selected obliged entity'** means a credit institution, a financial institution, or a group (…) which is under direct supervision by the Authority pursuant to Article 13; (2) 'Non-selected obliged entity' means a credit institution, a financial institution, or a group (…) other than a selected obliged entity;	

Tasks Article 5	
1) The Authority shall perform the following tasks with respect to ML/TF risks facing the internal market: (…) (a) (…) (b) (…) (c) collect and analyse information (…) on **weaknesses identified in the application of AML/CFT rules by obliged entities**, the risk exposure of obliged entities (…); (g) support, facilitate and strengthen cooperation and exchange of information between obliged entities and supervisors (…) 2) The Authority shall perform the following tasks with respect to selected obliged entities: (a) **ensure compliance of the selected obliged entities** with the requirements applicable to them pursuant to Regulation (EU) 2024/1624 and Regulation (EU) 2023/1113, (…) (b) carry out supervisory reviews and assessments at the level of individuals entities and at group wide level (…) and on the basis of [those] impose specific requirements, apply administrative measures and impose pecuniary sanctions (…).	The **AMLA is tasked with identifying systemic vulnerabilities across the entire market by analysing how obliged entities apply the rules** and where they are exposed to threats. For obliged entities chosen for direct oversight, the **AMLA as the primary regulator conducting detailed inspections and wielding the power to issue binding orders or fines to correct failures** and ensure the stability of the financial system.

AML/CFT supervisory methodology Article 8	
1) In cooperation with the supervisory authorities, the Authority shall develop and maintain an **up-to-date and harmonised AML/CFT supervisory methodology detailing the risk-based approach to supervision of obliged entities** in the Union. (…) 2) (…) The Authority shall **distinguish between obliged entities**, including on the basis of their activities and the type and nature of the ML/TF risk to which they are exposed. (…) 3) The Authority shall develop structured questionnaires (…) for the purposes of requesting, collecting, compiling and analysing data and information from obliged entities (…).	To replace the current patchwork of national rules, AMLA is required to build a **single unified playbook for how companies are supervised**. This methodology ensures that oversight is proportional to the actual risk a company poses, using standardised digital tools to gather objective data. **This approach prevents companies from being overwhelmed by inconsistent requests** while ensuring that supervisors across the Union have a comparable view of risks.
Central AML/CFT database Article 11	
2) The supervisory authorities shall transmit the following information, including the **data related to individual obliged entities (…)** (b) statistical information about the categories and the number of supervised obliged entities per category (…) and basic information about the **risk profile of those entities** **(c) the administrative measures applied and pecuniary sanctions imposed** in the course of supervision of individual obliged entities (…)	**A central intelligence hub is created to keep a comprehensive record of every company's compliance history.** By tracking risk profiles and past disciplinary actions, AMLA can identify trends and potential failures across Member States. **This collective data is essential for ensuring that when obliged entities operate in new markets, their past performance and the reputation of their management are known** to all relevant regulators.

Assessment of credit institutions and financial institutions for the purposes of selection for direct supervision Article 12	
1) (…) The Authority (…) shall carry out a **periodic assessment of credit institutions and financial institutions** (…) where they operate (…) in at least six Member States. 2) The supervisory authorities, and the **obliged entities subject to periodic assessment, shall supply the Authority with any information necessary** to carry out the periodic assessment (…). 3) **The inherent and residual risk profiles of an obliged entity assessed (…) shall be classified by the Authority as low, medium, substantial or high** (…).	This Article targets **institutions with a significant cross-border footprint for possible direct Union-level oversight. Obliged entities operating in six or more Member States** undergo a rigorous assessment of their 'residual risk', the risk that remains after their internal controls have been applied. This objective process classifies firms into risk categories, identifying those where Union-level supervision provides the most added value for the internal market.
The listing of selected obliged entities Article 13	
1) Credit institutions and financial institutions (…) whose **residual risk profile has been classified as high** pursuant to Article 12 shall qualify as selected obliged entities. 2) (…) where more than 40 entities are identified (…) the Authority may (…) agree on limiting the selection to a specific different number of entities or groups that is greater than 40. (…) 6) **A selected obliged entity shall remain subject to direct supervision by the Authority** until the Authority commences the direct supervision (…) based on a list established for the subsequent selection period (…).	**Obliged entities enter direct Union oversight classification as 'high risk' following the periodic assessment.** To ensure the system remains manageable, the Authority focuses on a core group of approximately 40 of the most significant firms. Once selected, these **obliged entities remain under the AMLA's direct supervision for at least three years**, providing stability and allowing for long-term improvements in their compliance frameworks.

Additional transfer of direct supervision tasks and powers in exceptional circumstances upon the request of a financial supervisor Article 14	
1) A financial supervisor may submit a reasoned request to the Authority for the Authority **to assume direct supervision** (…) with respect to a particular non-selected obliged entity. The request (…) shall only be submitted in **exceptional circumstances with the aim of addressing at Union level a heightened ML/TF risks or compliance failures** (…)	There is **a mechanism to handle crises in obliged entities that are not part of the regular selection list**. If an obliged entity suffers from extreme compliance failures or represents a systemic threat that national regulators cannot timely address, oversight can be transferred to the Union level. This ensures that **serious risks are met with a swift and specialised responses**, even if the obliged entity does not meet the standard size or geographic criteria for direct supervision.
Administrative measures Article 21	
1) (…) the Authority shall have the power to apply the administrative measures (…) to require any **selected obliged entity to take the necessary measures** where: (a) the **selected obliged entity is found to be in breach** of the Union acts (…) (b) the Authority has sufficient and demonstrable indications that **the selected obliged entity is likely to breach** (…) 2) (…) the Authority shall have (…) the power to apply the following administrative measures; (…) (b) **order obliged entities to comply**, including to implement specific corrective measures; (…) (e) **restrict or limit the business, operations or network** of institutions comprising the selected obliged entity, or require the divestment of activities; (…) (g) where a selected obliged entity is subject to authorisation, propose **the withdrawal or suspension of that authorisation**.	The **AMLA has a robust toolkit to force obliged entities back into compliance**. These measures are not just reactive; they can be **used pre-emptively if an obliged entity's internal procedure is deemed insufficient** for the risks it faces. By ordering specific changes to governance, restricting high-risk business activities, or even recommending the loss of an operating license, the AMLA ensures that obliged entities cannot profit from weak compliance.

Requests to act in exceptional circumstances following indications of serious, repeated or systematic breaches Article 32	
1) Financial supervisors shall notify the Authority where the situation of any **non-selected obliged entity (…) deteriorates rapidly and significantly** (…) or undermine the integrity of the Union's financial system. 2) The Authority may, where it has indications of **serious repeated or systematic breaches by a non-selected obliged entity,** request its financial supervisor to: (a) **investigate such indications** (…) (b) consider **imposing sanctions on that entity** (….)	Even for those institutions remaining under national oversight, AMLA acts as a high-level safeguard**. If an obliged entity's compliance deteriorates, AMLA can require national supervisors to open formal investigation or impose sanctions**, ensuring that they do not overlook systemic failures that could impact the broader Union.
Coordination and facilitation of the work of AML/CFT supervisory colleges in the non-financial sector Article 36	
1) The Authority shall (…) assist in the **setting up and functioning of AML/CFT supervisory colleges in the non-financial sector for obliged entity** (…) operating establishments in several Member States (…). 3) (…) the staff of the Authority shall **have full participation rights (…) including on-site inspections of obliged entities** in the non-financial sector (…)	Recognising that risks exist beyond banking, **AMLA coordinates supervisory colleges for cross-border obliged entities in the non-financial sector** (such as real estate or legal professions). These colleges allow regulators from different Member States to synchronise their oversight and conduct joint inspections, preventing obliged entities from exploiting gaps between national regimes and ensures consistent oversight across the Union.

Guidelines and recommendations Article 54	
1) The Authority shall (…) **issue guidelines and recommendations to (…) obliged entities.** 3**) Obliged entities shall make every effort to comply** with those guidelines and recommendations. (…) If required (…) **obliged entities shall report**, in a clear and detailed way, **whether they comply** with that guideline or recommendation.	AMLA uses guidelines and recommendations to provide **practical instructions on how the law should be applied**. While they are technically recommendations, **obliged entities are under a strong 'comply or explain' obligation**, ensuring that best practices are harmonised and that obliged entities are transparent about how they meet Union-level requirements.
Fees levied on selected and non-selected obliged entities Article 77	
1) The Authority **shall levy an annual supervisory fee on all selected obliged entities** (…) and on the **non-selected obliged entities that meet the criteria set out in Article 12 (1).** (…) 4) The Authority shall **communicate to the obliged entities concerned the basis for the calculation** of the annual supervisory fee.	To ensure **independent and sustainable oversight**, the supervisory system is funded by the firms that represent the greatest risk **and complexity**. These fees are calculated proportionally, ensuring that the **largest and most complex obliged entities** bear a fair share of the costs required to monitor the internal market.

Transparency International EU

31 Rue du Commerce, 1000 Brussels

http://www.transparency.eu/

+32 (0) 4 97 49 90 81

brussels@transparency.org

Transparency Register ID: 501222919
71