ACCOUNTANCY EUROPE.

NAVIGATING THE EU ANTI-MONEY LAUNDERING REGULATION

Key issues for the accountancy profession

Factsheet

FACTS.

ANTI-MONEY LAUDERING
DECEMBER 2024

HIGHLIGHTS

Accountants, auditors, and tax advisors play a crucial role in keeping European citizens safe from money laundering and terrorist financing.

In May 2024, the EU adopted an ambitious package of anti-money laundering (AML) reforms. The new legislation imposes strict AML obligations on accountants, auditors, tax advisors and other so-called 'obliged entities', significantly affecting their daily operations and compliance responsibilities.

This factsheet highlights the key changes introduced by the new AML Regulation and emphasises the importance of early preparation for these upcoming changes. It is the first in a series of papers and will be followed by factsheets on key issues for the accountancy profession arising from the 6th AML Directive and Regulation establishing a new AML Authority.

CONTENTS

INTRODUCTION

The new EU Anti-Money Laundering (AML) package is a major milestone in the EU's efforts to combat money laundering (ML) and terrorist financing (TF). The package includes the EU Single Rulebook Regulation, the 6th AML Directive, and a regulation establishing a new AML Authority (AMLA).

The AML Regulation (AMLR) will affect private sector actors, referred to as 'obliged entities', including accountants, auditors, and tax advisors. The AMLR will substantially impact their AML compliance obligations, including on targeted financial sanctions, customer due diligence, beneficial ownership transparency, suspicious activity reporting, and record retention. The new legislation also clarifies AML-related roles and responsibilities for obliged entity's senior management.

The AMLR is directly applicable to obliged entities unlike previous AML legislation that applied indirectly through national implementation. The AMLR will therefore minimise national variations for the first time, marking a significant step towards regulatory harmonisation. With directly applicable rules, the European Commission's (EC) goal is to ensure consistent enforcement of the AML legislation across the EU and to foster a more level playing field, especially with the creation of AMLA and the introduction of new supervisory rules.

OBJECTIVE

This factsheet summarises key provisions of the AMLR affecting the accountancy profession. It outlines main changes introduced by the AMLR[1] and emphasises the importance of early preparation. This publication is the first in a series and will be followed by additional factsheets addressing issues arising from the 6th AML Directive and the establishment of AMLA.

The new requirements will be implemented gradually, providing time for organisations to adjust their internal procedures to align with the new regulatory environment. In the coming years, AMLA will release specialised guidance and standards for both financial and non-financial sectors to enhance clarity and provide further detail into various aspects of the AMLR. We highlighted those specific areas across the document.

TIMELINE AND SCOPE

The legislation entered into force on 9 July 2024 and will begin applying on 10 July 2027. Entities subject to AML/CFT rules are known as 'obliged entities' under the AML legislation. They are required to implement AML/CFT measures, including conducting customer due diligence and reporting suspicious activities to Financial Intelligence Units (FIUs).

Obliged entities include nearly all financial institutions, such as banks, insurance companies, payment service providers, and investment firms, as well as various non-financial entities and professions. This latter category includes accountants, auditors, tax advisors, lawyers, notaries, real estate agents among others. The new rules have expanded the list of obliged entities to cover most of the crypto sector, crowdfunding service providers, traders of luxury goods, along with professional football clubs and agents.

Obliged entities should start preparing for the implementation of the new rules, ensuring that their AML/CFT frameworks are fully compliant. This includes updating internal policies, procedures and controls, strengthening customer due diligence, and enhancing monitoring and reporting mechanisms to meet the expanded obligations.

[1] This document provides a high-level summary of the key provisions that professional accountancy bodies and practitioners should, as a minimum, be aware of. It does not aim to give a comprehensive overview, nor can it be relied upon for legal compliance purposes. Readers are invited to refer directly to the AMLR legal text to ensure full compliance.

REQUIREMENTS FOR INTERNAL POLICIES, PROCEDURES AND CONTROLS

INTERNAL POLICIES, PROCEDURES AND CONTROLS, RISK ASSESSMENT AND STAFF

THE SCOPE OF OBLIGED ENTITIES' INTERNAL POLICIES, PROCEDURES AND CONTROLS[2]

Obliged entities should have in place an internal control framework consisting of policies, procedures and controls and a clear division of responsibilities throughout the organisation. These must be tailored to the entity's size, business nature, including its risks and complexity, and respond to ML/TF risks that the entity faces. They should include at least:

1. **internal policies and procedures** for business-wide risk assessment, risk management, customer due diligence, reporting suspicious activities, outsourcing, reliance on other entities' customer due diligence, record retention, and personal data processing (for the complete list, see Article 9 (2), AMLR)
2. **internal controls and an independent audit function**[3] to test the obliged entity's policies, procedures, and controls. This obligation appears to apply to all obliged entities irrespective of their size.

The management body in its management function[4] must approve the internal policies, while the compliance manager should approve the procedures and controls.

Obliged entities are required to keep these policies, procedures, and controls up to date and enhance them where weaknesses are identified.

By 10 July 2026, AMLA will issue guidelines on what obliged entities should consider when deciding on the extent of their internal policies, procedures and controls. Specifications are based on: 1) the nature of their business, including its risks and complexity; and 2) their size. Those guidelines will also identify situations where, due to the nature and size of the obliged entity:

- internal controls should be organised at the level of the commercial function, the compliance function and the audit function
- an external expert can carry out the independent audit function

BUSINESS-WIDE RISK ASSESSMENT[5]

As before, obliged entities must conduct a business-wide risk assessment to identify and evaluate their exposure to ML/TF risks.

Obliged entities must assess the associated ML/TF risks and implement measures to manage and mitigate those risks before launching new products, services, or business practices — such as new delivery channels, technologies, or entering new customer segments or geographical areas.

This risk assessment must be documented, regularly updated, and reviewed. The compliance officer should document the assessment, secure approval of the management body in its management function, and, if applicable, share it with the management body in its supervisory function[6].

---

[2] For further details, see Article 9.
[3] AMLR specifies that an external expert may carry out this test in case an obliged entity does not have an independent audit function.
[4] 'Management body in its management function' means the management body responsible for the day-to-day management of the obliged entity. See Article 2 (38), AMLR.
[5] For further details, see Article 10.
[6] 'Management body in its supervisory function' means the management body acting in its role of overseeing and monitoring management decision-making. See Article 2 (39), AMLR.

By 10 July 2026, AMLA will issue guidelines on the minimum requirements for the content of the business-wide risk assessment.

COMPLIANCE FUNCTIONS[7]

The AMLR introduces more comprehensive requirements for compliance functions compared to the rather limited coverage of this matter in the 4th AML Directive.

Obliged entities must appoint a member of the management body in its management function as a '**compliance manager**' to ensure implementation of the AMLR and ongoing compliance with the AML legislation. The compliance manager is responsible for making sure the obliged entity's internal policies, procedures, and controls align with its risk exposure and are properly implemented. This means that the compliance manager must ensure that sufficient human and material resources are allocated to that end. The compliance manager is also responsible for receiving information on significant weaknesses in these policies, procedures, and controls.

Obliged entities must also appoint a **compliance officer**, designated by the management body in its management function. This individual must hold a sufficiently senior position within the organisation. Compliance officer is responsible for the daily operation of AML/CFT policies, procedures, and controls, including implementing targeted financial sanctions, reporting suspicious activities to the FIU and acting as a contact point for competent authorities.

Depending on the obliged entity's size, risks, and complexity, the compliance manager and officer roles may be combined or shared with other duties, including across group entities if justified by size and low risk.

Obliged entities must:

- provide these compliance functions with resources, including staff and technology, proportionate to their size, nature, and risks
- empower them to propose necessary measures for effective internal policies, procedures and controls
- protect the compliance officer from retaliation, discrimination, and unfair treatment

The compliance officer and the person responsible for the independent audit function can report directly to the management body in its management function and, if it exists, to the management body in its supervisory function independently, and can raise concerns and warn the management body, where specific risk developments (may) affect the obliged entity.

The compliance officer can be dismissed only with prior notification of the management body in its management function. The obliged entity must also inform the supervisor of the compliance officer's removal and clarify whether the decision is related to the performance of their duties under the AMLR.

If the obliged entity is a natural person or a legal entity operated by a single individual, that person is responsible for performing all AML compliance tasks.

EMPLOYEE TRAINING[8]

Under the AMLR, the training obligation is more comprehensive than in the 4th AML Directive, which required training solely for obliged entity's employees involved in AML compliance. Now, obliged entities must ensure that all individuals involved in implementing AML/CFT measures—including employees, agents, and distributors—receive adequate training. The training should enable them to recognise potential ML/TF activities and know what steps to take when they encounter them.

[7] For further details, see Article 11.
[8] For further details, see Article 12.

PERIODIC EMPLOYEE ASSESSMENTS[9]

The AMLR introduces a new requirement mandating regular assessments for individuals responsible for an obliged entity's AML/CFT compliance. These individuals must be evaluated on their skills, knowledge, expertise, integrity, and conduct.

Furthermore, these employees must disclose any close personal or professional relationships with the entity's current or prospective customers to the compliance officer. To avoid conflicts of interest, such employees should be prevented from tasks related to compliance involving these customers.

SITUATION OF SPECIFIC EMPLOYEES[10]

The AMLR specifies that individuals who would normally qualify as obliged entities are not covered by its requirements when providing in-house services to businesses outside the AMLR's scope. Employees such as in-house lawyers or accountants are exempt from the AMLR obligations as these businesses are not gatekeepers of the EU's financial system.

Similarly, individuals performing activities covered by the AMLR are not considered obliged entities in their own right when these activities are conducted as part of their employment with an obliged entity. For example, lawyers or accountants working for a legal or accounting firm are not regarded as individual obliged entities themselves, but rather the firm as a whole is.

PROVISIONS APPLYING TO GROUPS

GROUP-WIDE REQUIREMENTS FOR PARENT UNDERTAKINGS[11]

A parent undertaking that is an obliged entity must ensure that all its branches and subsidiaries comply with the group's internal procedures, risk assessments, and staff requirements. To this end, the parent undertaking must perform a group-wide risk assessment that considers the risk assessments conducted by all branches and subsidiaries.

The parent undertaking must establish and implement group-wide policies, procedures, and controls, including on data protection and information sharing for AML/CFT purposes, and ensure employees are aware of regulatory requirements. Obliged entities within the group should adopt these group-wide policies, procedures and controls, considering their specificities and the risks to which they are exposed.

Compliance functions must be established at the group level, including a compliance manager and, if needed, a compliance officer. The compliance manager should regularly report to the parent undertaking's management body in its management function on the implementation of the group-wide policies, procedures and controls.

By 10 July 2026, AMLA will develop draft Regulatory Technical Standards, which will set out the minimum requirements of group-wide policies, procedures and controls including minimum standards for information sharing.

This will also cover the conditions under which the provisions related to group-wide requirements apply to entities within structures that share common ownership, management, or compliance control, including networks or partnerships. It will also address the criteria for identifying the parent undertakings for groups whose head office is located outside of the Union. Each obliged entity needs to assess whether their structure would fall under this provision.

[9] For further details, see Article 13.
[10] For further details, see Article 15.
[11] For further details, see Article 16.

OUTSOURCING OF AML/CFT TASKS[12]

The AMLR introduces new detailed rules on outsourcing of AML/CFT tasks, distinguishing it clearly from reliance on other obliged entities. Obliged entities may outsource AML/CFT-related tasks to service providers. However, the AMLR significantly tightened the conditions under which outsourcing is permitted compared to previous legislation.

Before outsourcing, the obliged entity must ensure that the service provider is qualified to perform the tasks and will comply with the obliged entity's policies and procedures. The terms for carrying out these tasks must be clearly defined in a contractual agreement between the obliged entity and the service provider. The ultimate responsibility for AML/CFT compliance remains with the obliged entity, which will be fully liable for any actions related to the outsourced tasks performed by service providers.

Certain critical tasks are prohibited to be outsourced. These are the following[13]:

a) proposal and approval of the business-wide risk assessment
b) approval of policies, procedures and controls
c) decisions on customer risk profiles
d) entering a business relationship
e) suspicious activities reporting
f) the approval of criteria to identify suspicious transactions.

The obliged entity must notify the supervisor about the outsourcing before the service provider starts the outsourced task. For each outsourced task, the obliged entity must be able to demonstrate to the supervisor that it understands the rationale behind the service provider's activities and the approach followed.

Obliged entities are not allowed to outsource AML/CFT tasks to service providers in high-risk third countries unless all the following conditions are met:

a) the service provider is part of the same group
b) the group complies with AML/CFT rules equivalent to those in the EU
c) this compliance is supervised at the group level by the home Member State's supervisory authority.

By 10 July 2027, AMLA will issue guidelines on the conditions under which outsourcing can take place as well as roles and responsibilities of the respective parties, supervisory approaches and expectations.

CUSTOMER DUE DILIGENCE

GENERAL PROVISIONS

CUSTOMER DUE DILIGENCE MEASURES[14] APPLICATION

Customer due diligence (CDD) is a cornerstone of an obliged entity's AML/CFT program. Through CDD, obliged entities gain a thorough understanding of their customers and the associated ML/TF risks.

Obliged entities must conduct CDD when they establish a business relationship with a new customer or when a customer seeks to conduct an occasional activity or transaction[15]. The AMLR has lowered the EU-wide

[12] For further details, see Article 18.
[13] For full details on these listed elements, see Article 18, AMLR.
[14] For further details, see Article 19.
[15] Article 19, AMLR provides a list of circumstances when the obliged entity is required to apply CDD measures:
a) establishing a business relationship

threshold for applying CDD on occasional transactions from EUR 15,000, as set by the 4th AML Directive, to EUR 10,000. AMLR also requires limited CDD measures for occasional transactions in cash amounting to a value of at least EUR 3,000.

AMLR sets out general CDD measures that must be applied for all customers, as well as specific "simplified" and "enhanced" due diligence measures that are determined by the level of risk posed by the customer.[16]

By 10 July 2026, AMLA will develop draft Regulatory Technical Standards which will provide details on:

a) the obliged entities, sectors or transactions that are associated with higher ML/TF risk and to which a value lower than EUR 10,000 applies
b) the related occasional transaction values
c) criteria to be considered for identifying occasional transactions and business relationships
d) the criteria to identify linked transactions

CUSTOMER DUE DILIGENCE MEASURES[17]

Obliged entities are required to carry out CDD on their customers, customers' beneficial owner or any person(s) acting on customers' behalf by applying all the following measures:

a) identify the customer and verify the customer's identity
b) identify the beneficial owners and take reasonable measures to verify their identity
c) understand the business relationship's or occasional transactions' purpose and intended nature
d) verify whether the customer or the beneficial owners are subject to targeted financial sanctions
e) assess and obtain information on the nature of the customer's business
f) conduct ongoing monitoring of the business relationship
g) determine if the customer or their beneficial owner is a politically exposed person, a family member[18] of one, or a close associate[19]
h) identify and verify the identity of anyone conducting a transaction or activity on the customer's behalf
i) verify that anyone acting on the customer's behalf is authorised and verify their identity

By 10 July 2026, AMLA will issue guidelines on the risk variables and factors that obliged entities should consider when establishing business relationships or conducting occasional transactions.

---

b) carrying out an occasional transaction of a value of at least EUR 10,000
c) participating in the creation of a legal entity, the setting up of a legal arrangement or, for (a) auditors, external accountants and tax advisors, (b) notaries, lawyers and other independent legal professionals, (c) trust or company service providers in the transfer of a legal entity's ownership
d) there is a suspicion of money laundering or terrorist financing
e) there are doubts about the veracity or adequacy of previously obtained customer identification data
f) there are doubts as to whether the person they interact with is the customer or person authorised to act on the customer's behalf.

Obliged entities must, at a minimum, identify and verify the customer's identity when conducting an occasional cash transaction of EUR 3,000 or more.

[16] The AMLR sets out a detailed list of lower and higher risk factors in Annex II and Annex III respectively.

[17] For further details, see Article 20.

[18] The definition of a 'family member' can be found in Article 2 (35), AMLR.

[19] AMLR defines a 'person known to be a close associate' as follows: (a) a natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person; (b) a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person. See Article 2 (36), AMLR.

INABILITY TO COMPLY WITH THE REQUIREMENT TO APPLY CUSTOMER DUE DILIGENCE MEASURES[20]

If an obliged entity cannot apply CDD measures as required, it must refrain from carrying out a transaction or establishing a business relationship. It should terminate the business relationship and consider reporting the case to the FIU.

The requirement to apply CDD measures does not apply in situations where auditors, accountants, tax advisors, and legal professionals are ascertaining their client's legal position or defending or representing their client in judicial proceedings. This exception does not apply if these obliged entities are involved in, facilitating, or aware that their client seeks legal advice for ML/TF purposes.

Obliged entities must document [21] their CDD actions, including decisions, supporting documents, and justifications. This also applies when they refuse or terminate a business relationship.

IDENTIFICATION AND VERIFICATION OF THE CUSTOMERS' AND BENEFICIAL OWNERS' IDENTITY[22]

Obliged entities must gather and verify customer identification details[23]:

- **for natural persons:** full name, place and full date of birth, nationalities, address, national and tax identification number (if applicable)
- **for legal entities:** name, legal form, office address, legal representatives' names, registration and tax numbers, names of persons holding shares or a directorship position

To identify a legal entity's beneficial owner(s)[24], obliged entities must collect all names, surnames, place and full date of birth, residential address, country of residence, nationality or nationalities, identity document number e.g. passport or national ID, unique personal identification number (if applicable), and a general description of this number's source.

If no beneficial owner(s) can be identified, a statement must be provided explaining why it was not possible to determine them. In that case, they must identify and verify senior management identity.

Verification can be done through ID documents or electronic means, and information on beneficial owners should be cross-checked with public and central registers.

TIMING OF CUSTOMER AND BENEFICIAL OWNER IDENTITY VERIFICATION[25]

Verification of the customer's and the beneficial owner's identity must take place before establishing a business relationship. However, if the ML/TF risk is assessed as low, this verification can be conducted during the establishment of the business relationship to avoid disrupting normal business operations.

REPORTING OF DISCREPANCIES[26]

The AMLR introduces stricter requirements for the reporting of discrepancies with information contained in beneficial ownership registers.

Obliged entities should consult central registers of beneficial ownership information ('central registers') to verify the accuracy of information obtained during CDD. These registers should not serve as the primary source for verification.

---

[20] For further details, see Article 21.
[21] Document retention period is covered below under section 'Data protection and record retention'.
[22] For further details, see Article 22.
[23] For further details including on the information to be collected for a trustee of an express trust or for other organisations that have legal capacity under national law, see Article 22, AMLR.
[24] Refer to the section below on 'Beneficial Ownership Transparency' for further details, including the threshold for determining ownership interest in a corporate entity.
[25] For further details, see Article 23.
[26] For further details, see Article 24.

Where obliged entities identify discrepancies between information in the central registers and the information they obtain from the customer or other reliable sources, they must report those discrepancies to the entity in charge of the relevant central register within 14 calendar days of detection.

When reporting discrepancies, obliged entities must accompany their reports with information they have indicating the discrepancy, identify who they believe the beneficial owners are, and, if applicable, the nominee shareholders and directors. Obliged entities may choose not to report discrepancies if they are limited to typographical errors, minor inaccuracies, or outdated data and instead request customers to correct them.

This requirement does not apply to auditors, external accountants, tax advisors, notaries, lawyers, and other independent legal professionals regarding information they obtain while ascertaining a client's legal position or defending or representing the client in legal proceedings. This exception does not apply if these obliged entities are involved in, facilitating, or aware that their client seeks legal advice for ML/TF purposes.

IDENTIFICATION OF THE PURPOSE AND INTENDED NATURE OF A BUSINESS RELATIONSHIP OR OCCASIONAL TRANSACTION[27]

CDD is not limited to the identification and verification of the customer's identity. An obliged entity must ensure it understands a business's purpose and intended nature before establishing a relationship or conducting an occasional transaction.

ONGOING MONITORING OF THE BUSINESS RELATIONSHIP AND CUSTOMERS' TRANSACTIONS[28]

Obliged entities must conduct ongoing monitoring of business relationships, including customer's transactions throughout the relationship. The goal is to ensure that these activities align with the obliged entity's knowledge of the customer, the customer's business activity, and their risk profile.

Additionally, obliged entities must ensure that the customer's documents, data, and information are kept up to date[29] as part of this ongoing monitoring process. The period between updates of customer information should correspond to the risk posed by the business relationship and should not exceed 1 year for higher risk customers and 5 years for all other customers.

Obliged entities are required to verify whether the customer or beneficial owner(s) are subject to targeted financial sanctions (TFS). For customers that are legal persons, the obliged entities must also verify if any natural or legal person subject to TFS controls the legal entity or have more than 50 % of the proprietary rights or holds a majority interest. If such circumstances are confirmed, the obliged entities will be subject to enhanced due diligence measures.

By 10 July 2026 AMLA will issue:

- guidelines on ongoing monitoring of a business relationship and on the monitoring of the transactions carried out in the context of such relationship
- draft Regulatory Technical Standards to provide further detail on the information necessary for the performance of standard, simplified and enhanced due diligence

By 10 July 2027, AMLA will issue guidelines defining the ML/TF risks, trends and methods involving any geographical area outside the EU to which obliged entities are exposed.

[27] For further details, see Article 25.
[28] For further details, see Article 26.
[29] Obliged entities must also review and update the customer information where:
a) there is a change in the relevant circumstances of a customer
b) the obliged entity has a legal obligation during the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owners
c) they become aware of a relevant fact which pertains to the customer.

SIMPLIFIED DUE DILIGENCE[30]

In low-risk situations, obliged entities may apply simplified due diligence (SDD) measures. This does not mean an exemption from CDD but rather a simplified or reduced set of scrutiny measures that still covers all aspects of the standard due diligence process. The SDD measures[31] mean:

a) verifying customer and beneficial owner identities within 60 days of establishing the business relationship, if justified by lower risk
b) reducing the frequency of customer identification updates
c) reducing the amount of information collected on the purpose and nature of the business relationship
d) reducing the frequency or scrutiny of customer transactions
e) applying other relevant SDD measures as identified by AMLA[32]

These SDD measures must be proportionate to the nature and size of the business and to the specific elements of lower risk identified. However, obliged entities must carry out sufficient monitoring of the transactions and business relationship to enable the detection of unusual or suspicious activities.

Obliged entities must regularly verify that the conditions for SDD still apply, with verification frequency based on the business's nature, size, and associated risks.

Obliged entities must not use SDD if:

a) they doubt the accuracy of the customer's information
b) lower-risk factors are no longer present
c) transaction monitoring indicates a higher risk, or
d) there is suspicion of ML, TF, or sanctions evasion

ENHANCED DUE DILIGENCE[33]

In higher-risk cases, obliged entities must apply enhanced due diligence (EDD) measures. When assessing ML/TF risks, obliged entities must consider the higher-risk factors listed in Annex III (AMLR), AMLA guidelines, and any other risk indicators, including FIU notifications and findings from the business-wide risk assessment under Article 10 (AMLR). This does not apply to cases related to 'high-risk third countries' covered in Articles 29-31 (AMLR).

The EDD measures include[34]:

a) gather additional information on the customer and beneficial owners
b) get additional information on the business relationship's nature and the source of funds and wealth
c) obtain information on the reasons for transactions and their alignment with the business relationship
d) get senior management approval for starting or continuing the relationship
e) closely monitor the business relationship by increasing the number and timing of controls

[30] For further details, see Article 33.
[31] For further details on these measures, see Article 33, AMLR.
[32] By 10 July 2026 AMLA will issue draft Regulatory Technical Standards to provide further detail on the information necessary for the performance of standard, simplified and enhanced due diligence. For details, see Article 28, AMLR.
[33] For further details, see Article 34.
[34] The full list of EDD measures can be found in Article 34, AMLR.

SPECIFIC PROVISIONS REGARDING POLITICALLY EXPOSED PERSONS[35]

In addition to the CDD measures, obliged entities must apply the following measures[36] for occasional transactions or business relationships with politically exposed persons (PEPs[37]):

a) obtain senior management approval
b) establish the source of wealth and funds
c) conduct enhanced ongoing monitoring

When a PEP is no longer in a prominent public function, obliged entities must assess the ongoing risk based on their former role. They must apply EDD measures for at least 12 months after the individual ceases to hold the function. This applies to occasional transactions or business relationships with former PEPs as well.[38]

Obliged entities must apply the same measures for occasional transactions or business relationships for PEP's family members[39] or known close associates as they do for PEPs themselves.

By 10 July 2027, AMLA will issue guidelines on criteria for identifying close associates and risk levels associated with PEPs, their family members, and close associates.

RELIANCE ON CUSTOMER DUE DILIGENCE PERFORMED BY OTHER OBLIGED ENTITIES

GENERAL PROVISIONS RELATING TO RELIANCE ON OTHER OBLIGED ENTITIES[40]

Obliged entities may rely on other obliged entities, within the EU or third countries, to fulfil CDD requirements laid down in Article 20(1), points (a), (b) and (c) provided that:

a) those entities apply AMLR CDD and record-keeping requirements, or AMLR equivalent in the case of third country obliged entities, and
b) their compliance with AML/CFT requirements is supervised in line with Chapter IV, 6th AML Directive

The ultimate responsibility for CDD compliance remains with the relying obliged entity.

When relying on CDD by obliged entities in third countries, the relying obliged entity must consider the geographical risk factors (see Annexes II and III, AMLR) along with guidance from the EC, AMLA, or other authorities.

For obliged entities that are part of a group, compliance with provisions relating to reliance on other obliged entities and related process can be ensured through group-wide policies, procedures and controls. Article 48(3) outlines the specific required conditions for this.

Obliged entities must not rely on entities in high-risk third countries. However, EU-based obliged entities may rely on their branches and subsidiaries in those countries if the conditions as laid out in Article 48(3) are met.

[35] For further details, see Article 42.
[36] For further details, see Article 42, AMLR.
[37] The PEPs list was expanded to include e.g. in a Member State - heads of regional and local authorities, including groupings of municipalities and metropolitan regions, with at least 50 000 inhabitants. For the full PEP definition, refer to Article 2, para 34, AMLR.
[38] For further details on measures for persons who cease to be politically exposed persons, see Article 45.
[39] AMLR specifies that, for the functions of heads of state, heads of government, ministers, deputy or assistant ministers, and equivalent roles at the Union level or in third countries, siblings are also considered 'family members'. See Article 2 (35, d).
[40] For further details, see Article 48.

PROCESS OF RELIANCE ON ANOTHER OBLIGED ENTITY[41]

Obliged entities must obtain all necessary CDD information (see points a, b and c in the section 'Customer due diligence measures' above) from the relied-upon entity, ensuring it provides, upon request, all the following[42]:

a) copies of customer identification data
b) supporting documents or sources used to verify identity, including electronic data
c) details on the purpose and nature of the business relationship

This information must be provided within 5 working days. The information transmission terms must be specified in a written agreement or, for group entities, in an internal procedure[43].

By 10 July 2027, AMLA will issue Guidelines for obliged entities on acceptable conditions for relying on another obliged entity's information, roles and responsibilities in such reliance cases, and supervisory approaches.

BENEFICIAL OWNERSHIP TRANSPARENCY

IDENTIFICATION OF BENEFICIAL OWNERS FOR LEGAL ENTITIES[44]

The AMLR refines the beneficial ownership definition. The revised definition is more comprehensive, providing a clearer framework for identifying individuals who ultimately own or control legal entities and arrangements.

Beneficial owners[45] of legal entities are the natural persons who:

a) hold direct or indirect ownership interest in the corporate entity, or
b) control the entity, directly or indirectly, through ownership interest or other means

AMLR indicates that 'control via other means' must be identified independently of, and in parallel to, ownership interest or control through ownership interest.

BENEFICIAL OWNERSHIP THROUGH OWNERSHIP INTEREST[46]

The threshold for determining ownership interest in a corporate entity is set at 25% or more of shares, voting rights, or other ownership interests, including rights to profits, internal resources, or liquidation balance. This applies to both direct and indirect ownership. AMLR clarifies that all shareholdings across all ownership levels must be considered.

Member States can identify categories of corporate entities exposed to higher ML/TF risks and propose a lower threshold to the EC, but it cannot be set below 15%.

BENEFICIAL OWNERSHIP THROUGH CONTROL[47]

Control over a legal entity can be exercised directly or indirectly through ownership interest or other means. The AMLR provides the following key definitions[48]:

[41] For further details, see Article 49.
[42] For further details, see Article 49.
[43] The conditions of such reliance are referred to in Article 49(5), AMLR.
[44] For further details, see Article 51.
[45] AMLR requires all legal entities in the EU to obtain and hold adequate, accurate and up-to-date beneficial ownership information. That information should be retained for 5 years and the identity of the person responsible for retaining the information should be reported to the central registers. For more, see Articles 62 and 63.
[46] For further details, see Article 52.
[47] For further details, see Article 53.
[48] For further details, see Article 53, para 2, AMLR.

- 'control' refers to the ability to significantly influence decisions within the entity
- 'indirect control' involves controlling intermediate entities in the ownership chain
- 'control through ownership' means holding 50% plus one of shares or voting rights

Control via other means can also involve majority voting rights, appointing/removing board members, veto rights, profit distribution decisions, or via formal/informal agreements, family ties, or nominee arrangements.[49]

REPORTING OBLIGATIONS

REPORTING OF SUSPICIONS[50]

Obliged entities must fully cooperate with the FIU by:

a) reporting when they know or suspect that funds or activities are linked to criminal activity or TF and responding to FIU requests for further information
b) providing the FIU with all requested information within the imposed deadlines

Obliged entities must respond to FIU requests within 5 working days. In justified and urgent cases, FIUs may reduce the deadline, even to less than 24 hours.

By 10 July 2026, AMLA will develop draft Implementing Technical Standards specifying the format to report suspicions.

By 10 July 2027, AMLA will issue guidelines on indicators of suspicious activity or behaviours, which will be periodically updated.

SPECIFIC PROVISIONS FOR REPORTING OF SUSPICIONS BY CERTAIN CATEGORIES OF OBLIGED ENTITIES[51]

Member States may permit certain professionals, like accountants, auditors, tax advisors to transmit information to a designated self-regulatory body[52], which must promptly forward it to the FIU.

Accountants, auditors, tax advisors, and similar professionals are exempt from the reporting obligation when receiving information while determining a client's legal position or representing them in judicial matters. This exemption does not apply if they are involved in or provide legal advice for ML, its predicate offenses, or TF, or if they know the client seeks advice for these purposes.

PROHIBITION OF DISCLOSURE[53]

Obliged entities, their directors, and employees must not inform customers or third parties that their activities are under assessment or that information has been or will be shared with authorities for ML/TF analysis. This restriction does not apply to disclosures to competent authorities, self-regulatory bodies performing supervisory functions, or for the purposes of investigating and prosecuting ML/TF and other criminal activities.

For accountants, auditors, tax advisors, and similar professionals, disclosure is allowed between these obliged entities or third-country entities, if they operate within the same legal structure or group, which shares common ownership, management or compliance control, including networks or partnerships.

[49] For further details, see Article 53, AMLR.
[50] For further details, see Article 69.
[51] For further details, see Article 70.
[52] Further details about self-regulatory bodies can be found in the 6th AML Directive.
[53] For further details, see Article 73.

INFORMATION SHARING

EXCHANGE OF INFORMATION IN THE FRAMEWORK OF PARTNERSHIPS FOR INFORMATION SHARING[54]

Obliged entities may participate in information-sharing partnerships for CDD and suspicious activity reporting (SAR) purposes. They are required to notify their supervisory authorities about their intention to join. Compliance with EU and national laws remains the responsibility of each participant.

Information shared within a partnership must be limited to essential customer details, including their identity, the purpose and nature of their business relationship, transaction information, risk factors, and any ML/TF suspicions.

Obliged entities must adhere to specific conditions[55] when sharing information within partnerships, such as:

a) record all instances of information sharing within the partnership
b) not rely solely on the information received in the context of the partnership to comply with the AMLR
c) assess shared information before making decisions impacting the customer relationship. If shared information leads to refusing or terminating a relationship, document the decision and note a partnership as the information source
d) conduct their own assessments of ML/TF risks
e) share info only for customers with higher ML/TF risks or when more info is needed

Obliged entities participating in information-sharing partnerships must establish clear policies and procedures for information sharing.

DATA PROTECTION AND RECORD RETENTION

PROCESSING OF PERSONAL DATA[56]

Obliged entities may process special categories of personal data and data related to criminal convictions if necessary to prevent ML/TF, and must follow these specific safeguards[57]:

a) customers must be informed that such data may be processed for AML compliance purposes
b) data must be from reliable sources, accurate, and up to date
c) decisions must not result in biased or discriminatory outcomes
d) high-level security measures, especially confidentiality, must be implemented

RECORD RETENTION[58]

Obliged entities must retain all of the following[59]:

a) copies of CDD documents
b) records of their customer's activity assessments and any resulting suspicious activity reports
c) supporting evidence and transaction records
d) documents and records from information-sharing partnerships

[54] For further details, see Article 75.
[55] For the complete list of conditions which apply for information sharing see Article 75, AMLR.
[56] For further details, see Article 76.
[57] For further details, see Article 76.
[58] For further details, see Article 77.
[59] For further details, see Article 77.

Information must be kept for 5 years after ending a business relationship, completing a transaction, or refusing to engage with a customer. After 5 years, personal data must be deleted unless authorities request an extension, which can be up to an additional 5 years.

PROVISION OF RECORDS TO COMPETENT AUTHORITIES[60]

Obliged entities must have systems to promptly and securely respond to their FIU or other competent authorities' inquiries about past or current business relationships within the last five years, ensuring confidentiality.

LIMITS TO LARGE CASH PAYMENTS IN EXCHANGE FOR GOODS OR SERVICES[61]

Persons trading in goods or services can accept or make cash payments up to EUR 10,000 (or equivalent), whether in single or linked transactions. Member States may set lower limits.

Exceptions include payments between individuals not acting in a professional capacity and payments/deposits at financial institutions, which must report amounts above the limit to the FIU within specified deadlines.

[60] For further details, see Article 78.
[61] For further details, see Article 80.

Avenue d'Auderghem 22-28, 1040 Brussels

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 49 professional organisations from 35 countries that represent close to **1 million** professional accountants, auditors and advisors. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18).