ACCOUNTANCY EUROPE.

6TH ANTI-MONEY LAUNDERING DIRECTIVE

Key issues for accountancy professionals

Factsheet

FACTS.

ANTI- MONEY LAUNDERING

MARCH 2026

HIGHLIGHTS

In May 2024, the EU adopted a comprehensive package of anti-money laundering (AML) reforms. The 6th Anti-Money Laundering Directive, alongside the AML Regulation and the Regulation establishing a new AML Authority, is a key part of this overhaul.

Accountants, auditors, and tax advisors play a vital role in keeping European citizens safe from money laundering and terrorist financing. This factsheet outlines the most relevant changes introduced by the 6AMLD for the accountancy profession. It follows our first factsheet on the AML Regulation.

While the Directive is primarily addressed to Member States and national supervisors, it directly shapes how AML rules are interpreted, enforced, and operationalised. It sets out supervisory powers, responsibilities, and engagement with obliged entities, meaning it has real, day-to-day practical implications for accountants, auditors, and tax advisers.

Understanding this evolving supervisory landscape is essential for compliance, effective risk management, and preparation for increasingly coordinated supervisory scrutiny across the EU.

CONTENTS

INTRODUCTION

The new EU Anti-Money Laundering (AML) package marks a major milestone in the EU's ongoing efforts to combat money laundering (ML) and terrorist financing (TF). It consists of three core components:

- AML Regulation (AMLR)
- 6th Anti-Money Laundering Directive (6AMLD) and
- Regulation establishing the Anti-Money Laundering Authority (AMLA).

Accountancy Europe is publishing a series of factsheets highlighting key aspects of this new AML package that are relevant for professional accountants, auditors and tax advisors to help its members prepare[1] for the new legislation.

This factsheet focuses on the main changes introduced by the 6AMLD[2]. It follows our first factsheet on the AML Regulation.

SCOPE AND FOCUS OF THE 6AMLD

While the AML Regulation (AMLR) sets out obligations for private-sector obliged entities, the 6AMLD focuses on the institutional and organisational responsibilities of Member States and national supervisory authorities. It establishes **minimum standards for supervision, sanctions, cooperation, and information-sharing across the EU**. Specifically, the 6AMLD sets out rules on:

- measures applicable to sectors exposed to ML and TF, at national level
- registration and checks on senior management and beneficial owners of obliged entities
- ML/TF risks identification at the EU and Member State levels
- creation and access to beneficial ownership, bank account, and real estate information
- requirements for residence rights in exchange for investment
- responsibilities and tasks of Financial Intelligence Units (FIUs)
- responsibilities of bodies supervising obliged entities
- cooperation between competent authorities and other EU authorities.

WHY DOES THIS DIRECTIVE MATTER FOR ACCOUNTANCY PROFESSIONALS?

Although the 6AMLD is primarily targeted at Member States, national supervisors, and FIUs, it has **direct relevance for the accountancy profession** and other obliged entities because its implementation determines how AML rules such as the ones set out in the AMLR are interpreted and enforced in practice. Accountancy Europe briefing paper *5 ways the 6AMLD will impact accountants and auditors* provides a practical overview of how the 6AMLD will affect their day-to day work.

The Directive sets the framework within which national supervisors will operate, including their powers, responsibilities, and how they engage with obliged entities. For example, **supervisors are empowered to inspect compliance systems, assess risk exposure, evaluate internal controls, and apply sanctions**.

These supervisory tasks inevitably shape **what is expected of accountants when fulfilling their AML duties**, especially around risk assessment, reporting, and internal governance. Understanding the evolving

[1] See also Accountancy Europe paper - *New EU AML rules: advice for accountancy practitioners* (2025).
[2] 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 6AMLD legal text to ensure full compliance.

supervisory architecture and institutional expectations at a more holistic level is essential to effective compliance.

The Directive also introduces **significant new provisions related to self-regulatory bodies**, mandating Member States to ensure these bodies are subject to oversight by a public authority.

Importantly, the Directive establishes **new supervisory structures for cross-border professional networks**. National supervisors must set up AML/CFT supervisory colleges when non-financial obliged entities, such as accounting or tax advisory firms, operate across multiple Member States. These colleges will coordinate supervision, facilitate information-sharing, and promote consistent enforcement of AML obligations across the EU. Accountants working internationally or under special national authorisation regimes should expect **closer oversight and more structured cooperation among authorities**.

A solid understanding of the institutional and supervisory landscape will help obliged entities enhance compliance readiness, sharpen risk awareness to effectively navigate the increasingly coordinated regulatory environment. Accountants must therefore keep pace with evolving supervisory expectations to manage compliance risks, update internal policies, and respond effectively to supervisory inquiries or inspections.

APPLICATION TIMELINE

The 6AMLD entered into force on 9 July 2024 and will apply from 10 July 2027.

It repeals and replaces the 4th[3] and 5th AML Directives, refocusing EU AML/CFT policy on institutional effectiveness and consistent implementation across Member States.

As a Directive, it requires transposition into national law[4] – mostly by 10 July 2027, though some provisions may have earlier or later deadlines depending on the article.

RISK ASSESSMENTS

UNION-WIDE RISK ASSESSMENT[5]

Under the 4th AML Directive (4AMLD), the EC was required to carry out a supranational risk assessment (SNRA) every two years, focusing specifically on ML and TF risks that affected the internal market and cross-border activities. These assessments identified common methods used by criminals and flagged sectors or products that were vulnerable.

The 6AMLD raises the bar. It considerably **expands both the SNRA scope and structure**. The Commission is now mandated not only to assess ML and TF risks, but also to evaluate **risks of non-implementation and evasion of targeted financial sanctions** at both the EU (supranational) and national levels. This is a major addition for firms, since sanctions compliance is increasingly tied to AML/CFT controls.

In addition, while 4AMLD required a biennial reporting cycle, 6AMLD introduces a longer but more stable four-year cycle. The first updated SNRA must be drawn up by 10 July 2028, and thereafter every four years, though the Commission retains the flexibility to publish interim updates if needed.

---

[3] The 4th AML Directive (Directive (EU) 2015/849) is repealed with effect from 10 July 2027.

[4] Member States are required to bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 10 July 2027 and immediately inform the Commission (Article 78, 6AMLD).
However, for Amendments to 4th AML Directive (Directive (EU) 2015/849), Article 74, the deadline is 10 July 2025; for Articles 11, 12, 13, and 15, it's 10 July 2026; and for Article 18, it's 10 July 2029. They must also inform the Commission immediately. Member States must communicate to the Commission the main national laws they adopt related to this Directive.

[5] For further details, see Article 7, 6AMLD.

Another important change is **the level of detail**. Under 6AMLD, the SNRA must drill down into risks by sector, product, cross-border and third-country risk exposure, and it must look closely at vulnerabilities linked to legal persons and arrangements, including foreign structures.

Finally, 6AMLD strengthens how these findings feed into practice. Member States must designate competent authorities or mechanisms to coordinate their response to the identified risks, ensure that national risk assessments take account of the supranational report, and be ready to update national or sectoral assessments if new risks are identified.

NATIONAL RISK ASSESSMENT[6]

In addition to the above-mentioned EU-wide risk assessment, the Directive also requires each Member State to conduct and regularly update a national risk assessment to identify and address risks related to ML, TF, and the risks of non-implementation and evasion of targeted financial sanctions. The assessment must be reviewed at least every four years, with more frequent or sector-specific reviews if needed.

Each Member State must designate an authority or set up a mechanism to coordinate its response to ML and TF risks and inform the Commission about this.

When conducting national risk assessments, Member States must take into account the Union-level risk report outlined in the previous section, including the sectors, products, and findings it covers.

Member States should use their national risk assessments to:

a) improve AML/CFT regimes, especially by identifying areas where obliged entities must apply enhanced measures
b) identify sectors or areas of higher or lower ML/TF risk
c) assess ML/TF risks linked to domestic and foreign legal persons and arrangements
d) prioritise resources to counter ML/TF and sanctions evasion
e) set sector-specific rules based on risk levels
f) share relevant risk information promptly with authorities and obliged entities.

In the national risk assessment, Member States are also required to describe their institutional AML/CFT structure, cooperation mechanisms, and resources allocated.

AML/CFT-RELATED STATISTICS[7]

Each year, Member States must send the Commission and AMLA key data on their AML/CFT systems — including sector size, STRs, investigations, prosecutions, convictions, confiscations, FIU performance, supervisory actions, beneficial ownership and bank account register use, and how financial sanctions are applied.

From July 2030, the EC will publish an EU-wide report every two years, explaining the figures and making them available online.

BENEFICIAL OWNERSHIP REGISTERS

CENTRAL BENEFICIAL OWNERSHIP REGISTERS[8]

The Directive requires Member States to ensure that beneficial ownership information is stored in a central register. This information must be machine-readable and comply with relevant regulations. Under the previous

[6] For further details, see Article 8, 6AMLD.
[7] For further details, see Article 9, 6AMLD.
[8] For further details, see Article 10, 6AMLD.

AML rules, Member States already maintained central registers of beneficial ownership. However, verification standards varied, and registers mainly relied on reporting by companies and obliged entities.

6AMLD gives the power to entities in charge of the central registers[9] to request all necessary information from legal entities, trustees, and beneficial owners to identify and verify their beneficial owners. These bodies are now responsible not only for recording beneficial ownership information but also for verifying its accuracy, requesting supporting documentation, and imposing penalties for non-compliance. This represents a shift from the previous framework, which relied more heavily on obliged entities to validate beneficial ownership.

The beneficial ownership information includes corporate documents such as board resolutions, meeting minutes, partnership agreements, trust deeds, and related contracts.

If no beneficial owner is identified, the central register must include:

a) a statement confirming the absence or inability to determine a beneficial owner, with a justification, and
b) details of all senior managing officials of the legal entity[10].

The information on the absence or inability to determine a beneficial owner must be available to competent authorities, AMLA for joint analyses, self-regulatory bodies, and obliged entities. However, obliged entities can access the statement only if they report a discrepancy or prove efforts to identify the beneficial owner, in which case they can also access the justification.

By 10 July 2028, the Commission will issue recommendations on how entities responsible for central registers should verify beneficial ownership information, and how obliged entities and competent authorities should identify and report discrepancies.

Entities in charge of central registers must verify **whether any beneficial ownership information they hold relates to persons or entities subject to targeted financial sanctions**. Where a legal entity, its controller, or any of its beneficial owners is subject to such sanctions, the register must clearly indicate this. The indication must be visible to all users of the register and remain in place until the sanctions are lifted.

Entities in charge of the central registers must take appropriate action to resolve reported discrepancies in beneficial ownership information within 30 working days of notification by a competent authority or obliged entity. Where the information can be verified, it must be corrected. A note on the discrepancy must remain visible in the register until it is resolved.

The entity in charge of the central register must have the power, either directly or through application to another authority, including judicial authorities, to conduct checks, including on-site inspections at the business premises or registered office of legal entities. These checks aim to establish the current beneficial ownership and verify that the submitted information is accurate, adequate, and up to date. Its right to verify this information must not be restricted, obstructed, or precluded.

Entities in charge of central registers must be able to request necessary information from other registers, including in third countries.

They are also empowered to impose sanctions, including fines, for repeated failures to provide accurate and up-to-date beneficial ownership information.

Central registers, interconnected via the European Central Platform, must retain beneficial ownership data for five years after the dissolution of a legal entity or arrangement. Member States may extend this period by up to five years for crime prevention or prosecution if deemed necessary and proportionate. Personal data must be deleted after the retention period expires.

---

[9] The “entity in charge of the central register” refers to the public authority designated by each Member State. They function as supervisory and enforcement authorities for beneficial ownership information.
[10] For further details, see Article 10 (5), 6AMLD.

ACCESS BY COMPETENT AUTHORITIES, SELF-REGULATORY BODIES AND OBLIGED ENTITIES[11]

Competent authorities must have immediate, unfiltered, and free access to interconnected central registers without alerting the legal entity concerned. Access must also be granted to self-regulatory bodies, tax authorities, national authorities for Union restrictive measures, AMLA, EPPO, OLAF, Europol, and Eurojust.

Member States may choose to provide obliged entities access to beneficial ownership information in central registers for a cost-recovery fee only, ensuring that charges do not restrict effective or timely access.

ACCESS FOR PERSONS WITH LEGITIMATE INTEREST[12]

Member States must grant access to beneficial ownership information to individuals or entities that can demonstrate a legitimate interest in preventing and combating ML and TF. This includes details such as the beneficial owner's name, month and year of birth, nationality, country of residence, and the nature and extent of the beneficial interest. Access should primarily be provided electronically, with alternative formats available if needed.

The Directive now clarifies and defines **categories of natural or legal persons deemed to have a legitimate interest**, for example:

- journalists and media professionals investigating financial or economic crime
- civil society organisations and academia involved in AML/CFT activities
- persons or entities entering into transactions with legal entities, seeking to avoid exposure to financial crime risks[13].

These categories formalise and clarify access compared with the earlier, purely case-by-case approach under AMLD4. The change reflects the CJEU's 2022 ruling, which reinstated the legitimate-interest requirement following the annulment of blanket public access under AMLD5.

In addition, Member States must grant case-by-case access to any other persons able to demonstrate a legitimate interest in preventing and combating ML and TF.

EXCEPTIONS TO THE ACCESS RULES TO BENEFICIAL OWNERSHIP REGISTERS[14]

Member States should provide for an exemption from access to all or part of beneficial ownership information in exceptional cases where disclosure would expose the beneficial owner to a disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence, or intimidation. An exemption should also apply if the beneficial owner is a minor or legally incapable.

Exemptions require case-by-case evaluation and guarantee administrative and judicial review. Annual exemption statistics must be published and reported to the Commission. This article does not apply to notaries, lawyers, and other independent legal professionals that are public officials.

[11] For further details, see Article 11, 6AMLD.
[12] For further details, see Article 12, 6AMLD.
[13] For the complete list, see Article 12, 6AMLD.
[14] For further details, see Article 15, 6AMLD.

FINANCIAL INTELLIGENCE UNITS

A Financial Intelligence Unit (FIU) is a national authority, or in some cases a centralised body shared between countries. It acts as the link between those legally required to report suspicious transactions or activities — such as banks, payment service providers, accountants, lawyers, real estate agents, and other regulated professionals — and law enforcement or prosecuting authorities. The FIU collects reports of unusual or suspicious transactions, analyses them to identify possible ML or TF and passes its findings to the competent authorities for investigation or further action.

Under the 6AMLD, FIUs' core role of receiving, analysing, and sharing suspicious transaction reports remains unchanged. The Directive gives them clearer legal powers, stricter deadlines, and stronger tools to access and use information. They can now also instruct banks, payment providers, or other regulated professionals to closely monitor a particular account or transaction pattern and report the results, alongside enhanced cross-border cooperation and new safeguards like a Fundamental Rights Officer.

ALERTS TO OBLIGED ENTITIES[15]

FIUs must alert obliged entities about information relevant to customer due diligence, including:

a) high-risk transactions or activities
b) high-risk individuals
c) high-risk geographic areas.

FIUs must annually provide obliged entities with strategic information on typologies, risk indicators, and trends in ML and TF.

FEEDBACK BY FIU[16]

The Directive requires **FIUs to provide obliged entities**[17] **with annual feedback** on suspicion reports covering the information quality, timeliness, suspicion descriptions, and submitted documentation. This feedback does not intend to cover every report submitted by obliged entities.

FIUs are also obliged to share feedback with supervisors for risk-based supervision.

The Directive mandates FIUs to report annually to AMLA on the feedback given to obliged entities and provide statistics on suspicious transaction reports submitted by the categories of obliged entities.

By 10 July 2028, AMLA will issue best practice recommendations for feedback, including type and frequency.

CONFIDENTIALITY OF REPORTING[18]

FIUs are required:

- to have in place mechanisms to protect the identity of obliged entities, their employees, and related persons who report suspicions under Article 69(1)(a) of the AML Regulation
- not to disclose the source of reports when responding to requests for information from competent authorities or sharing analysis results.

[15] For further details, see Article 26, 6AMLD.
[16] For further details, see Article 28, 6AMLD.
[17] Feedback must be provided to the individual obliged entity or to groups or categories of obliged entities, taking into consideration the overall number of suspicious transactions obliged entities reported.
[18] For further details, see Article 36, 6AMLD.

ANTI-MONEY LAUNDERING SUPERVISION

POWERS AND RESOURCES OF NATIONAL SUPERVISORS[19]

The Directive requires Member States to ensure **effective supervision of all obliged entities** and appoint one or more supervisors to ensure compliance with the AML Regulation and the Transfer of Funds Regulation.

If a Member State requires special authorisation for an obliged entity from another country to operate in its territory under the freedom to provide services, it must also ensure that those activities are supervised by its national supervisors — even if the services are provided remotely. This supervision must be communicated to the supervisor in the country where the obliged entity's head office is located.

Supervisors must have sufficient financial, human, and technical resources to carry out their duties. Their staff must be appropriately skilled, act with integrity, and uphold professional standards, including confidentiality, data protection, and managing conflicts of interest.

For auditors, accountants, tax advisors, and similar professionals, Member States may allow self-regulatory bodies to supervise these obliged entities, provided they possess the necessary powers, resources, and qualified staff.

If a Member State assigns supervision of a category of obliged entities to multiple supervisors, it must ensure consistent and efficient supervision across the sector. To achieve this, the Member State must either appoint a lead supervisor or set up a coordination mechanism.

If all obliged entities are supervised by multiple supervisors, the Member State must establish a coordination mechanism involving all supervisors. This must include:

a) the public authority (under Article 52, 6AMLD) if supervision is handled by a self-regulatory body
b) a lead supervisor, if appointed, when a category of obliged entities has several supervisors. If no lead is appointed, supervisors must designate a representative.

The national supervisors are required to perform the following tasks:

a) disseminate relevant information to obliged entities in line with Article 39 (6AMLD)
b) decide on those cases where sector-specific risks are clear and understood, making individual documented risk assessments under Article 10 of the AML Regulation unnecessary
c) verify the adequacy and implementation of obliged entities' internal policies, procedures, controls and resource allocation
d) assess and monitor ML/TF risks, and the risks of non-implementation and evasion of targeted financial sanctions the obliged entities are exposed to
e) monitor obliged entities' compliance with their obligations in relation to targeted financial sanctions
f) conduct necessary off-site investigations, on-site inspections, thematic checks, and other inquiries or assessments to verify obliged entities' compliance with the AML Regulation and administrative measures under Article 56 of this Directive
g) take appropriate supervisory measures to address breaches by obliged entities identified during supervisory assessments and follow up on the implementation of those measures.

Supervisors must have sufficient powers to perform their tasks including the power to:

a) request information from obliged entities and outsourced service providers for compliance checks under the AML Regulation and the Transfer of Funds Regulation
b) apply administrative measures, including pecuniary sanctions, to address breaches.

[19] For further details, see Article 37, 6AMLD.

PROVISION OF INFORMATION TO OBLIGED ENTITIES[20]

Supervisors must provide information on ML and TF to the obliged entities they supervise. This information must include:

a) the EU-level risk assessment by the EC (as per Article 7) and related recommendations
b) national or sector-specific risk assessments (in line with Article 8)
c) guidelines, recommendations, and opinions issued by AMLA under Articles 54 and 55 of the AMLA Regulation
d) information on third countries identified under Chapter III, Section 2 of the AML Regulation
e) guidance and reports from AMLA, other supervisors, public authorities overseeing self-regulatory bodies, the FIU, other competent authorities, international organisations, or standard setters. This includes information on ML/TF methods relevant to a sector, indicators for identifying suspicious transactions or activities, and guidance on obligations related to targeted financial sanctions.

Supervisors must conduct outreach activities, as needed, to inform obliged entities of their obligations.

Supervisors must immediately provide obliged entities with information on persons or entities designated under targeted financial sanctions and UN financial sanctions.

RISK-BASED SUPERVISION[21]

Under the 4AMLD, competent authorities were already required to adopt a risk-based approach in supervising obliged entities. This meant that supervisors needed to focus their resources on areas, sectors, or entities deemed to carry higher ML/TF risks. At the same time, the 4AMLD left much of the implementation and methodology to national discretion, with limited guidance on standardising risk assessment or supervisory intensity across different sectors or Member States. Cross-sectoral coordination and the systematic use of intelligence from FIUs were encouraged but not fully formalised.

By contrast, the **6AMLD strengthens and formalises the risk-based approach**. Supervisors are now explicitly required to identify, assess, and categorise risks across all obliged entities in a systematic way, applying supervisory measures proportionate to the level of risk. Higher-risk entities are subject to closer scrutiny, while lower-risk ones may face lighter oversight, introducing **the concept of supervisory intensity**.

The 6AMLD also emphasises cross-border cooperation and coordination with the AMLA to ensure consistent application of risk-based supervision across the EU. Furthermore, the directive encourages supervisors to leverage data, intelligence, and analyses from FIUs to refine risk assessments and prioritise interventions more effectively.

By 10 July 2026, AMLA must develop and submit draft Regulatory Technical Standards (RTS) to the Commission. These standards must:

- define benchmarks and methodology for assessing and classifying inherent and residual risk profiles of obliged entities
- specify how often these risk profiles must be reviewed
- take into account major events, operational changes, nature, and size of the business.

By 10 July 2028, AMLA must issue guidelines for supervisors on:

- characteristics of risk-based supervision
- internal measures, including staff training

[20] For further details, see Article 39, 6AMLD.
[21] For further details, see Article 40, 6AMLD.

- steps for conducting risk-sensitive supervision.

Supervisors should consider the level of discretion exercised by obliged entities and appropriately assess the underlying risk assessments, as well as the adequacy of their internal policies, procedures, and controls.

The 6 AMLD requires supervisors to prepare an annual activity report, with a public summary that includes:

a) categories and number of obliged entities supervised
b) description of their supervisory powers, tasks, and coordination mechanisms in which they participate
c) overview of supervisory activities.

AML/CFT SUPERVISORY COLLEGES IN THE NON-FINANCIAL SECTOR[22]

CREATION OF NON-FINANCIAL AML/CFT SUPERVISORY COLLEGES

The concept of "AML/CFT supervisory colleges" is formalised and significantly expanded under 6AMLD. The Directive requires **non-financial supervisors in charge of the parent undertaking of a group of obliged entities in the non-financial sector, or of the head office of an obliged entity to establish dedicated AML/CFT supervisory colleges** in any of the following cases:

a) when an obliged entity in the non-financial sector or a group has establishments in at least two other Member States besides the one where its head office is located
b) when a third-country entity (not a credit or financial institution) that is subject to AML/CFT requirements has establishments in at least three Member States.

This also **applies to structures with shared ownership, management, or compliance control, including networks or partnerships**, where group-wide requirements under Article 16 of the AML Regulation apply.

The permanent **members of such a college** should be:

- the non-financial supervisor in charge of the parent undertaking or head office, and
- the non-financial supervisors in charge of establishments in host Member States, or for supervision of the obliged entity in other Member States under Article 37(1), second subparagraph (6AMLD)[23].

IDENTIFICATION OF CROSS-BORDER NON-FINANCIAL OBLIGED ENTITIES AND COORDINATION AMONG SUPERVISORS

Non-financial supervisors should identify:

a) all non-financial obliged entities with their head office in their Member State that have establishments in other Member States or third countries
b) all establishments set up by those obliged entities in other Member States or third countries
c) all branches or offices that non-financial obliged entities from other Member States or third countries have set up in their territory.

When non-financial obliged entities operate in other Member States under the freedom to provide services, the non-financial supervisor from the home Member State may invite the supervisors from those other Member States to join the college as observers.

[22] For further details, see Article 50, 6AMLD.
[23] When an obliged entity operates cross-border under specific authorisation regimes and is supervised by the host country — those host supervisors must also be part of the college.

ESTABLISHMENT OF AML/CFT SUPERVISORY COLLEGES WITH THIRD-COUNTRY PARTICIPATION AND PROTECTION OF LEGAL PRIVILEGE

Member States may permit the creation of AML/CFT supervisory colleges when a non-financial obliged entity established in the EU has establishments in at least two third countries. Non-financial supervisors may invite their counterparts in those third countries to set up the college. The participating non-financial supervisors must create a written agreement outlining the conditions and procedures for cooperation and information exchange.

If the AML/CFT supervisory college includes auditors, external accountants, tax advisors, notaries, lawyers, or other independent legal professionals or their groups, the written agreement must include procedures to prevent the sharing of information protected under Article 21(2)[24] of the AML Regulation, which covers legal professional privilege. This restriction does not apply where the exceptions in Article 21(2)[25], second subparagraph are met.

FUNCTIONS AND OBJECTIVES OF AML/CFT SUPERVISORY COLLEGES

Colleges should be used for exchanging information, providing mutual assistance, and coordinating the supervisory approach to a group or obliged entity. This includes, where relevant, taking appropriate and proportionate measures to address serious breaches of the AML Regulation and the Transfer of Funds Regulation that occur at the group or entity level, or across their establishments in the jurisdiction of any supervisor participating in the college.

PARTICIPATION IN THE AML/CFT SUPERVISORY COLLEGES

AMLA may attend AML/CFT supervisory colleges meetings as an observer and should help facilitate their work.

Non-financial supervisors may allow third-country counterparts to participate in AML/CFT supervisory colleges as observers in these situations:

- a third-country entity that is subject to AML/CFT requirements has establishments in at least three Member States, or
- EU non-financial obliged entities or groups have branches or subsidiaries in those third countries.

Participation is subject to these conditions:

a) third-country counterpart requests participation and all college members agree, or the college invites the counterpart
b) EU data protection rules on data transfers are respected
c) third-country counterpart signs the written agreement (see Article 50(7), 6AMLD) and shares relevant supervisory information within the college
d) shared information is protected by professional secrecy rules equivalent to Article 67(1), 6AMLD and is only used for supervisory purposes.

The non-financial supervisor in charge of the group's parent undertaking, head office, or the college must assess whether these conditions are met before allowing the third-country counterpart to join. They must

[24] AMLR: Article 21(2): Paragraph 1 shall not apply to notaries, lawyers, other independent legal professionals, auditors, external accountants and tax advisors, to the extent that those persons ascertain the legal position of their client, or perform the task of defending or representing that client in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.
[25] AMLR: Article 21(2): The first subparagraph shall not apply when the obliged entities referred to therein: (a) take part in money laundering, its predicate offences or terrorist financing; (b) provide legal advice for the purposes of money laundering, its predicate offences or terrorist financing; or (c) know that the client is seeking legal advice for the purposes of money laundering, its predicate offences or terrorist financing; knowledge or purpose may be inferred from objective factual circumstances.

submit the assessment to the permanent college members and may repeat it when needed. AMLA may assist in this assessment.

If the permanent members of the college consider it necessary, they may invite additional observers, as long as confidentiality requirements are complied with. These observers may include FIUs.

If college members disagree on the measures to take regarding an obliged entity, they may ask AMLA for assistance. AMLA must give its opinion within 2 months.

REGULATORY TECHNICAL STANDARDS AND PERIODIC REVIEW OF AML/CFT SUPERVISORY COLLEGES

By 10 July 2026, AMLA must draft and submit to the EC RTS specifying:

a) general conditions for how AML/CFT supervisory colleges in the non-financial sector function, including cooperation terms with permanent members and observers
b) the template for the written agreement non-financial supervisors must sign under Article 50(7), 6AMLD
c) conditions for third-country non-financial supervisors to participate
d) additional measures required when the group includes credit or financial institutions.

By 10 July 2029, and every 2 years after that, AMLA must issue an opinion on how AML/CFT supervisory colleges in the non-financial sector are functioning. The opinion must include:

a) an overview of the colleges set up by non-financial supervisors
b) an assessment of the actions taken by those colleges and the level of cooperation achieved, including any difficulties encountered in their functioning.

OVERSIGHT OF SELF-REGULATORY BODIES[26]

The Directive introduces an important new provision for the accountancy sector regarding the oversight of self-regulatory bodies. **Where a Member State allows a self-regulatory body to supervise auditors, external accountants, tax advisers, notaries, or other independent legal professionals** (under Article 37(3), 6AMLD), **it must ensure that the activities of that body in the performance of such function are subject to oversight by a public authority**. Under the previous rules, oversight of such self-regulatory bodies by a public authority was not a regulatory requirement and was left to the discretion of each Member State.

The public authority overseeing self-regulatory bodies must ensure an **adequate and effective supervisory system for those non-financial obliged entities**. This includes:

a) checking that any self-regulatory body (performing or intending to perform supervision) meets the requirements in Article 37(3), 6AMLD
b) issuing guidance on how those functions should be performed
c) ensuring the adequate and effective performance of supervisory functions
d) reviewing any exemptions granted by self-regulatory bodies from the requirement to prepare an individual documented risk assessment (as per Article 37(5)(b))
e) regularly informing self-regulatory bodies of relevant AMLA activities or tasks, especially regarding peer reviews under Article 35 of the AMLA Regulation.

This public authority must also have the necessary powers to carry out its responsibilities. At a minimum, it should have the power to:

a) request any information needed to monitor compliance and perform checks
b) instruct a self-regulatory body to fix failures in performing its duties or to prevent such failures.

[26] For further details, see Article 52, 6AMLD.

The authority must take into account any relevant guidance it or AMLA has issued when giving instructions.

It must operate free from undue influence, and its staff must:

- follow professional secrecy rules equivalent to those in Article 67, 6AMLD
- maintain high standards of confidentiality, data protection, and integrity, and
- apply procedures to prevent and manage conflicts of interest.

Effective, proportionate, and dissuasive measures or sanctions may be applied if a self-regulatory body fails to comply with a request, instruction, or other action taken by the public authority under paragraph 2 or 3, Article 52, 6AMLD.

The public authority overseeing self-regulatory bodies must promptly inform the authorities responsible for investigating and prosecuting criminal offences, either directly or through the FIU, of any breaches subject to criminal sanctions that it identifies while carrying out its tasks.

The authority must publish an annual report that includes:

a) the number and type of breaches identified by each self-regulatory body, along with any financial penalties or administrative measures applied to obliged entities
b) the number of suspicious transaction reports submitted to the FIU by obliged entities under each self-regulatory body either directly (under Article 69(1) of the AML Regulation or via the self-regulatory body (under Article 70(1) of that Regulation)
c) the number and type of penalties or other measures imposed by each self-regulatory body to ensure compliance with the AML Regulation, as referenced in Article 55(1) of this Directive
d) the number and type of actions taken by the public authority itself, including instructions issued to self-regulatory bodies.

The report must be published on the authority's website and submitted to the Commission and AMLA.

PECUNIARY SANCTIONS AND ADMINISTRATIVE MEASURES

GENERAL PROVISIONS[27]

Obliged entities can be held liable for breaches of the AML Regulation and the Transfer of Funds Regulation. Member States must ensure supervisors can apply sanctions that are effective, proportionate, and dissuasive. Where supervisors cannot impose sanctions directly, they may apply to judicial authorities, provided the outcome is equivalent; such Member States must notify the Commission by 10 July 2027.

Sanctions must be enforceable not only against legal persons but also senior management or other responsible individuals. Supervisors must also inform criminal authorities when breaches may constitute criminal offences.

Pecuniary sanctions and administrative measures may be imposed by:

a) supervisors directly
b) supervisors together with other authorities
c) other authorities acting under supervisors' responsibility
d) judicial authorities, on application by supervisors.

[27] For further details, see Article 53, 6AMLD.

Supervisors must consider all relevant factors when setting sanctions or administrative measures, including breach severity and duration, repetition, responsibility, financial capacity, gains or losses, cooperation, and prior breaches.

Legal persons are liable for breaches of AML Regulation or the Transfer of Funds Regulation committed by senior personnel acting on their behalf or benefiting them, including failures to supervise subordinates.

By 10 July 2026, AMLA must submit draft RTS to the EC covering breach severity indicators, criteria for sanctions, and methodology for periodic penalties, and issue Guidelines on base sanction amounts by breach type and entity category.

PECUNIARY SANCTIONS[28]

Under the Directive, **obliged entities must be subject to pecuniary sanctions for serious, repeated, or systematic breaches, whether intentional or due to negligence**, of the following provisions of the AML Regulation:

a) Chapter II (Internal policies, procedures, and controls)
b) Chapter III (Customer due diligence)
c) Chapter V (Reporting obligations)
d) Article 77 (Record retention).

Pecuniary sanctions must also be possible where obliged entities fail to comply with administrative measures under Article 56 of this Directive, or commit breaches that are not serious, repeated, or systematic.

In the above listed cases (a-d), the **maximum pecuniary sanction must be at least**:

- twice the benefit gained from the breach (if this can be determined), or
- EUR 1,000,000, whichever is higher.

While **the Directive sets minimum thresholds for maximum pecuniary sanctions**, **Member States may allow authorities to impose higher amounts**, provided the entity's ability to pay is considered.

ADMINISTRATIVE MEASURES[29]

Supervisors must be able to apply administrative measures to an obliged entity in the following cases:

a) **breaches of the AML Regulation** or the Transfer of Funds Regulation, either in combination with pecuniary sanctions for serious, repeated and systematic breaches, or on their own
b) **weaknesses in the obliged entity's internal policies, procedures, or controls** that could lead to breaches of the above Regulations, and where administrative measures can help prevent or reduce that risk
c) when **the entity's internal policies, procedures or controls are not proportionate** to its ML, related predicate offences or TF risks.

Supervisors must have the power at least to:

a) issue recommendations
b) order obliged entities to comply, including by taking specific corrective measures
c) issue a public statement which identifies the natural or legal person and the nature of the breach

[28] For further details, see Article 55, 6AMLD.
[29] For further details, see Article 56, 6AMLD.

d) order a person to stop the misconduct and not repeat it

e) restrict or limit the business, operations, or network of the obliged entity, or require it to stop certain activities

f) suspend or withdraw the entity's authorisation, if applicable

g) require changes to the governance structure.

Supervisors must also be able to use the administrative measures to:

a) request any data, documents, or information needed to carry out their tasks without delay, and impose additional or more frequent reporting requirements

b) require the obliged entity to strengthen its internal policies, procedures, and controls

c) require the obliged entity to apply specific rules or policies for high-risk clients, transactions, activities, or delivery channels

d) order actions to reduce ML or TF risks linked to the obliged entity's activities or products

e) temporarily ban any person responsible for a breach or in a managerial role from holding management positions in obliged entities.

The administrative measures must include binding deadlines for implementation, where appropriate. Supervisors must follow up and assess whether the obliged entity has carried out the required actions.

Supervisors may also be given the power to apply other types of administrative measures beyond those listed above.

PUBLICATION OF PECUNIARY SANCTIONS, ADMINISTRATIVE MEASURES AND PERIODIC PENALTY PAYMENTS[30]

Supervisors must publish decisions on pecuniary sanctions, key administrative measures (Article 56(2)(c)-(g), 6AMLD), and periodic penalty payments on their website. Publications must include the type/nature of breach, identity of those responsible, and sanction amounts (unless investigatory or certain exceptions apply).

Supervisors may delay, anonymise, or skip publication if it risks market stability, ongoing investigations, or is disproportionate.

Published decisions must remain online for 5 years; personal data for no more than 5 years and only as needed.

REPORTING OF BREACHES AND WHISTLEBLOWER PROTECTION[31]

The Whistleblower Directive applies to the reporting of breaches of the AML Regulation and the Transfer of Funds Regulation and of this Directive, and to the protection of persons reporting such breaches and of the persons concerned by those reports.

The 6AMLD mandates supervisory authorities to set up external reporting channels and follow up on reports concerning obliged entities.

The public authorities overseeing self-regulatory bodies (under Article 52, 6AMLD) must set up external reporting channels and handle reports from those self-regulatory bodies and their staff, where these relate to how they carry out their supervisory duties.

[30] For further details, see Article 58, 6AMLD.
[31] For further details, see Article 60, 6AMLD.

Non-financial supervisors must report annually to AMLA on the number and status of whistleblower reports received, the types of irregularities reported, actions taken or planned, and reasons for dismissals without revealing the identity or details of the reporting persons.

COOPERATION AND EXCHANGE OF CONFIDENTIAL INFORMATION

COOPERATION IN RELATION TO AUDITORS[32]

Supervisors in charge of auditors, public authorities overseeing self-regulatory bodies, FIUs, and public authorities competent for overseeing statutory auditors and audit firms under Article 32 of the Statutory Audit Directive and Article 20 of the Audit Regulation must cooperate closely and exchange information relevant to their functions.

Confidential information must be used solely for tasks under this Directive or related EU legislation.

Member States may restrict such cooperation if it would interfere with ongoing investigations, analyses, or legal proceedings.

PROFESSIONAL SECRECY REQUIREMENTS[33]

All persons working or who have worked for supervisors, public authorities (including those overseeing self-regulatory bodies), and auditors or experts acting on their behalf are bound by professional secrecy.

Confidential information obtained in the course of supervisory duties may only be disclosed in summary or aggregate form, unless required for criminal investigations or shared with FIUs.

The Directive allows the exchange of such information between supervisors including AMLA, FIUs, competent authorities including self-regulatory bodies, and financial supervisors provided it is used strictly for fulfilling their AML/CFT or related regulatory responsibilities, including in legal proceedings.

EXCHANGE OF INFORMATION AMONG SUPERVISORS AND WITH OTHER AUTHORITIES[34]

The 6AMLD strengthens and formalises provisions relating to the cross-border supervisory cooperation and information exchange. It requires Member States to authorise the exchange of information between:

a) supervisors and public authorities overseeing self-regulatory bodies, whether located in the same or different Member States
b) supervisors and financial market authorities in relation to their respective supervisory duties
c) supervisors responsible for auditors, and where relevant, public authorities overseeing self-regulatory bodies, with the authorities responsible for statutory auditors and audit firms as defined in the Statutory Audit Directive and the Audit Regulation, including cross-border cooperation.

Professional secrecy obligations under Article 67(1) and (3) do not prevent these exchanges. However, shared confidential information may only be used for the authorities' official duties or in administrative/judicial proceedings directly related to those duties, and must always be subject to equivalent confidentiality safeguards.

[32] For further details, see Article 65, 6AMLD.
[33] For further details, see Article 67, 6AMLD.
[34] For further details, see Article 68, 6AMLD.

Rue de la Loi 62 (temporary), Brussels, 1040, Belgium

accountancyeurope.eu

+32(0)2 893 33 60

Accountancy Europe

accountancyeurope.bsky.social

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).