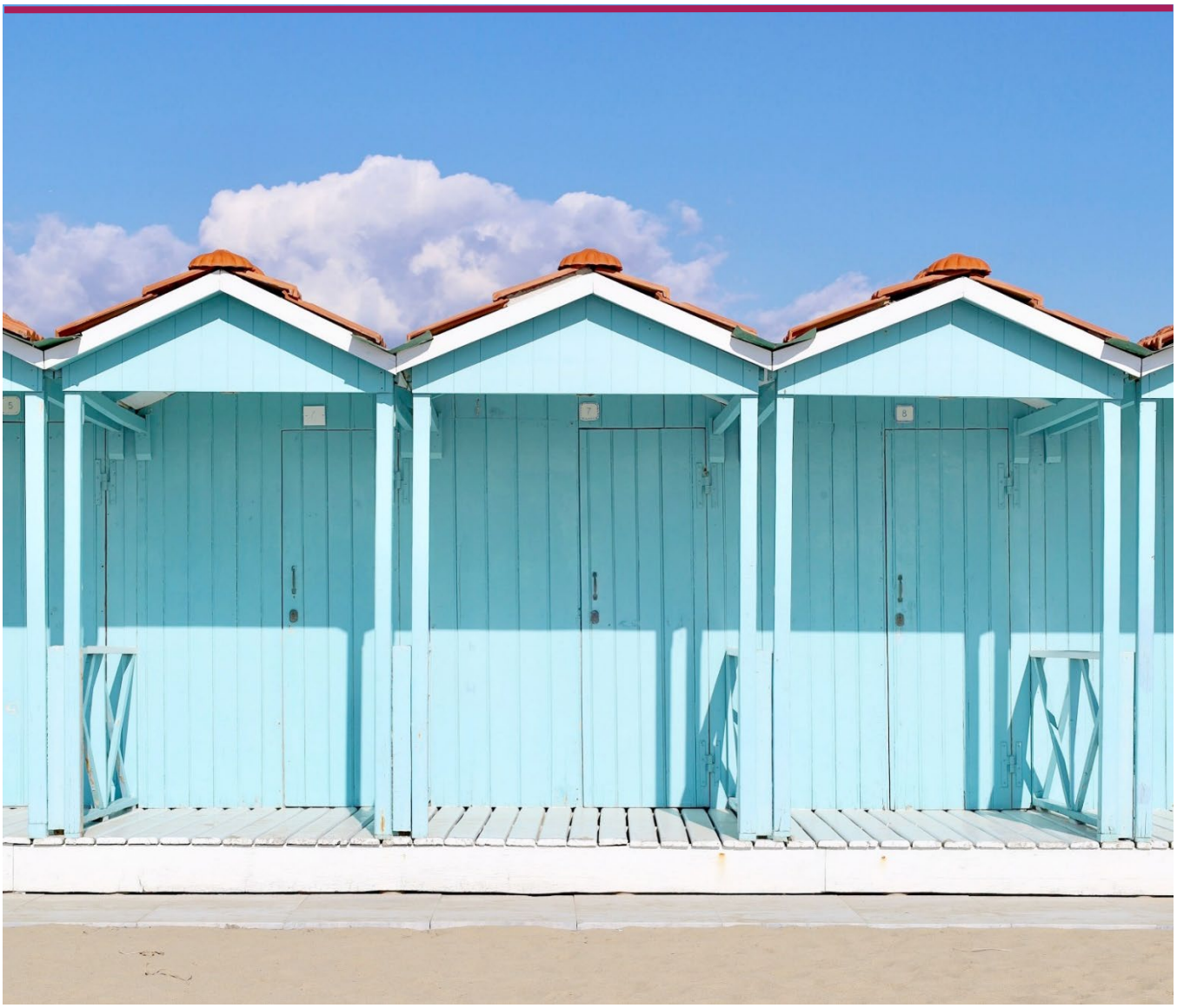
SUMMARY

EU Anti-Money Laundering Rules



Executive Summary

This section gives a high-level view of what the Anti-Money Laundering Package contains, what is new and the timetable for implementation.

1

1.1 Overview

The EU Anti-Money Laundering Package (the "AML Package") is an overhaul of the EU's existing anti-money laundering ("AML"), countering the financing of terrorism ("CFT") and beneficial ownership reporting rules. The AML Package is targeted at financial and non-financial entities considered to be at greater than usual risk of being exploited by criminals for money laundering or terrorist financing purposes.

In doing this, the EU is reflecting the recommendations[1] made by the Financial Action Taskforce ("FATF"), the international anti-money laundering standards-setting body. However, the AML Package is not a direct transposition of the FATF Recommendations. All jurisdictions which abide by FATF standards implement them in a way they deem to be proportionate to address the risks identified. This means the rules may vary among jurisdictions around the world. A key aim of the AML Package is to make AML/CFT practices across the EEA[2] more uniform.

1.2 New and changed requirements

The AML Package contains some significant new requirements and amendments to existing ones. This summary explains what they are and from when they apply, where that is clear.

The new and amended rules include:

- Stricter and more detailed requirements for identifying and verifying who beneficial owners are;
- Inclusion of AIFMs[3] and UCITS management companies[4] as obliged entities in their own right;
- Where a collective investment undertaking has no legal personality, responsibility for reporting beneficial ownership information with respect to the fund is placed on the collective investment undertaking's manager;
- Extra reporting requirements by obliged entities to supervisors and between supervisors;
- Expansion of the scope of the requirements to include crypto-assets, crypto- asset services and crypto-asset service providers ("CASPs");

---

1 *See* the 40 recommendations made by the FATF. FATF, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" (updated November 2023), available at https://www.fatf-gafi.org/en/topics/fatf-recommendations.html (the "FATF Recommendations").

2 Directives and regulations apply to all members of the European Economic Area ("EEA"), not just full members of the EU. The EEA included the 27 EU member states plus Iceland, Liechtenstein and Norway as of the date this summary was published.

3 Article 4(1)(b) of the Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, as amended ("AIFMD").

4 Article 2(1)(b) of Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities, as amended (the "UCITS Directive").

- Stronger and clearer requirements for internal compliance procedures and staff training;
- More detail on the requirements for doing business with third country entities and outsourcing to third country service providers;
- A new category of "selected obliged entity" for larger firms that operate across EEA Member States and create higher than usual risks;
- More detailed requirements on customer due diligence, including requirements for when there should be enhanced due diligence, as well as when simplified due diligence is appropriate;
- Greater detail on requirements for cross-border operations; and
- The new European supervisory body, the Anti-Money Laundering Authority ("AMLA"), which will set up a new central database, make Union-wide risks assessments and directly supervise "selected obliged entities".

1.3 The AML Package explained

The AML Package is made up of three separate pieces of legislation:

- The EU Anti-Money Laundering Regulation ("AMLR");[5]
- The sixth EU Anti-Money Laundering Directive ("AMLD6");[6] and
- The EU Anti-Money Laundering Authority Regulation ("AMLAR"),[7] which, among other things, establishes the AMLA.

Each of these is described below. All three cross-refer extensively to each other.

AMLR

The AMLR puts in place what are intended to be more consistent or harmonised rules in all EEA jurisdictions ("Member States"). All EU regulations such as the AMLR are directly applicable, which means that they apply to all Members States without the need for them to be transposed into each Member State's local laws and rules. This is often referred to as the "Single European Handbook".[8]

The AMLR sets out the revised list of "obliged entities", i.e., the entities and individuals within scope of the rules (see discussion in **Section 2.1** of this summary), and their duties. Key among the duties assigned to obliged entities are identifying the beneficial

5 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

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

7 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.

8 Regulations are used when the intention is to be sure that all Member States apply particular rules in uniform manner.

owners of assets, carrying out varying levels of due diligence on customers ("CDD") and reporting relevant information to national regulators' beneficial ownership registries. National regulators then send relevant information to the new AMLA central database and share it, where justified, with other national regulators.

It also sets out cooperation requirements with respect to financial intelligence units ("FIUs")[9] and cross border requirements.

AMLD6

AMLD6 updates the requirements that Member States must meet under their duties to prevent money laundering and terrorist financing and changes to the rules applicable to FIUs.

AMLD6's aim is to improve the organisation of national AML regulatory systems and set out clear rules on how FIUs and supervisors, including national supervisors, such as banking and securities authorities, and the AMLA are expected to work together.

AMLAR and the AMLA

The AMLAR contains the rules which create the AMLA, an entirely new pan-European supervisory authority. It will take over the existing powers of the European Banking Authority ("EBA") in relation to AML and CFT matters,[10] in addition to having new coordination duties, running a new central database and supervising selected obliged entities operating on a cross-border basis. The AMLA will be based in Frankfurt am Main, Germany.

1.4 Timeline

The new requirements take effect over a range of different dates, reflecting the need for certain preparatory steps, for example, to set up and staff the AMLA, to take place before the new requirements apply.

The table below sets out the key dates for different elements of the AML Package to come into effect. This includes rules to be transposed into national law and the responsibilities that have to be transferred to different bodies. In addition to these deadlines, the AML Package contains implementing measures which empower the AMLA and the European Commission to develop further guidance. The table identifies ones AIMA members are likely to care about that are due to be published by 10 July 2027. There are also many other implementing measures that are due to be published both before and after that date. All of the implementing measures are described briefly in Annex 1, along with their respective deadlines.

Key Events	Date
AMLR, AMLD6 and AMLAR published in the Official Journal	19 June 2024
AMLAR effective date	26 June 2024

[9] A country's national body charged with collecting information on suspicious or unusual activity is that country's FIU.

[10] The EBA will continue to exist albeit with an amended remit.

Key Events	Date
European Commission's authority to commence operation of AMLA started	26 July 2024
AMLR and AMLD6 effective date	9 July 2024
Main bulk of AMLAR begins to apply	1 July 2025
European Commission authority over AMLA activities ends and AMLA stand-alone operations begin	31 December 2025
Implementing Measures for AMLR Articles 9(4), 10(4), 16(4), 17(3) and (4), 19(9), 20(3), 28(1), 68(2), 69(3) and 81(1) and AMLD6 Articles 31(2) and (3), 40(2), 41(2), 46(4), 49(14), 50(13) and 53 are due	10 July 2026
Transposition deadline for certain AMLD6 Articles regarding access to beneficial ownership registers	10 July 2026
Implementing Measures for AMLR Articles 18(8), 21(4), 32(1), 34(5), 37(3), 40(2), 42(2), 50 and 69(5) are due	10 July 2027
AMLR begins to apply	10 July 2027
Transposition deadline for remaining AMLD6 Articles	10 July 2027

1.3 Structure of this summary

Because many of the requirements in the new AMLR, AMLD6 and AMLAR overlap, this summary looks at the relevant areas of the AML Package by theme rather than listing the individual requirements of each piece of legislation in turn.

These themes are as follows:

- Scope, which now includes CASPs, internal controls, revised tasks for asset managers and staffing considerations (**Chapter 2**);
- Updates to beneficial ownership identification (**Chapter 3**);
- Due diligence and know your customer requirements (**Chapter 4**);
- Information sharing, reliance on third parties/outsourcing, cross border activities and third country entities (**Chapter 5**); and
- Supervision, including the new AMLA and FIUs, reporting, data sharing and beneficial ownership register requirements (**Chapter 6**).

This summary assumes the reader has a baseline knowledge of the current requirements and focuses on the new requirements rather than touching everything in the AML Package.

AIMA's on-going engagement

The publication of the Package has fired the starting gun for the preparation and approval of a host of implementing measures. These must be formulated by the AMLA and the European Commission over the timeline described in Annex 1. AIMA will be engaging closely with this work to ensure forthcoming requirements and guidance is meaningful, necessary, cost-effective and proportionate for members.

If you would like to participate in this work or get further details please contact AIMA Director, Asset Management Regulation, James Hopegood at jhopegood@aima.org.

Scope and Internal Controls

The AML Package brings more financial assets and institutions into scope, changes the internal controls and is more explicit about the staffing requirements for those controls.

2

2.1 In-scope "obliged entities"

The types of entities from the asset management and funds industry which are categorised as obliged entities are:

- Collective investment undertakings, which are defined as AIFs[11] and UCITS[12] and their respective AIFMs and UCITS management companies;[13]
- Investment firms[14] as defined by MiFID 2;
- Crypto-asset service providers ("CASPs"),[15] crypto-asset services,[16] crypto-assets[17] and self-hosted addresses[18] as defined by the MiCA and Travel Rule regulations;
- Central securities depositaries[19] as defined by CSDR;
- Financial mixed activity holding companies where there is at least one credit institution or financial institution within a group;
- Trust or company service companies; and
- Auditors, external accountants and tax advisers, lawyers, notaries and other legal professionals carrying out a range of services.

This summary focuses on requirements applicable to entities in the first four categories above. Insurance companies, insurances intermediaries, e-money institutions, crowdfunding service providers and intermediaries, estate agents and mortgage and credit brokers are also in scope as financial institutions but are not otherwise covered by this summary.

Selected obliged entities

Some obliged entities will be assessed as large enough to have an EU-wide impact, and will be directly supervised by AMLA. These so-called "selected obliged entities" will be assessed using the relevant one of a series of benchmarks.[20]

The benchmarks use the following factors:

- Customer related risks:
    - The share of non-resident customers from third countries; and

11 Article 4(1)(a) of the AIFMD.
12 Article 1(2) of the UCITS Directive.
13 *See* AMLR Article 2 (Definitions)(6)(e)(i) and (ii).
14 Article (4)(1)(1) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, as amended ("MiFID 2").
15 Article 3(1)(15) of Regulation (EU)2023/1114 (the "MiCA Regulation").
16 Article 3(1)(16) of the MiCA Regulation.
17 Article 3(1)(5) of the MiCA Regulation.
18 Article 3(20) of Regulation 2023/1113 (the "Travel Rule").
19 Article 2(1)(1) of Regulation (EU) 909/2014, as amended ("CSDR").
20 *See* AMLAR Article 12 (Assessment of credit institutions and financial institutions for the purposes of selection for direct supervision) and AMLAR Article 13 (The listing of selected obliged entities).

- The share of customers who are political exposed persons ("PEPs").

- Products and services offered based on:
  - The relative trading volume of products and services identified as most vulnerable to money laundering/terrorist financing risks; and
  - The relative volume of products, services and transactions offering a "considerable level" of protection to client privacy, identity or other form of anonymity.

- Geographical factors:
  - The annual volume of correspondent banking and crypto-asset services provided by EEA financial sector entities in their countries; and
  - The number and share of correspondent banking and crypto-asset clients in third countries.

According to the AMLAR, it is anticipated that no more than 40 obliged entities will be categorised as selected obliged entities.[21]

2.2 Internal organisation, controls and tasks

The AMLR sets out a range of requirements for obliged entities to have in place written internal policies, procedures and controls to tackle money laundering and terrorist financing threats. There are also requirements on how they carry out risk assessments and for staff and their training. The policies, procedures and controls should be proportionate to the nature of obliged entities' businesses, risks and complexity.

Internal policies, procedures and controls

More detail has been added to the required internal policies, procedures and controls which apply not just to employees but also to agents, distributors and service providers. The new or more detailed requirements for what must be included in an obliged entity's policies, procedures and controls[22] include:

- Carrying out and updating the business-wide risk assessment;
- Maintaining the risk management framework;
- Customer due diligence (see **Section 3** of this summary), including procedures to determine whether the customer, the beneficial owner or the person on whose behalf or for the benefit of whom a transaction or activity is being conducted is a PEP or a family member or person known to be a close associate;
- Reporting of suspicious transactions;
- Outsourcing and reliance on customer due diligence performed by other obliged entities;

[21] See AMLAR Recital 26.

[22] Although a number of these obligations existed before, they were not expressly required to be a part of the obliged entity's policies, procedures and controls.

- Record retention and policies in relation to the processing of personal data;
- Monitoring and managing compliance with internal policies and procedures, identifying and managing deficiencies and remedying them;
- Checking that new staff with certain tasks and functions as well as agents and distributors are of good repute and verifying that existing staff with certain tasks and functions and existing agents and distributors are also of good repute;
- Internal communication of the internal policies, procedures and controls, including to staff, agents, distributors and service providers involved in the implementation of the AML/CFT policies; and
- A policy for training employees and, where relevant, agents and distributors on AML/CFT requirements.

There should be an audit function in place to test these policies and controls. This can be done by an external expert. The internal policies should be reviewed regularly.[23]

Risk assessment

Obliged entities must now take account of the new EU-wide risk assessment the AMLA will have to carry out, as well as the findings from the existing national regulator assessments of EEA jurisdictions and the European Commission's third country assessments. Further details of these other assessments are set out in **Section 5**.

The business-wide risk assessment requirements applicable to obliged entities have been maintained and supplemented with more detail.[24] For example, obliged entities now have an explicit duty to factor in AML and CFT risks before launching new products, services and when developing new delivery channels and using new or evolving technologies.

The obliged entity must also refer to an indicative list of variables (see Boxes 1 to 3 below) which set out the issues and risk factors to be considered when determining whether something is lower risk or higher risk.[25] These must be used for both risk assessments and CDD.

Box 1 -- Risk variables (AMLR Annex I)

Customer risk variables

- The customer's and the customer's beneficial owner's business or professional activity;
- The customer's and the customer's beneficial owner's reputation;
- The customer's and the customer's beneficial owner's nature and behaviour;
- The jurisdictions in which the customer and the customer's beneficial owner are based;

23 *See* AMLR Article 9 (Scope of internal policies, procedures and controls).
24 *See* AMLR Article 10 (Business-wide risk assessment).
25 *See* AMLR Annexes I to III.

- The jurisdictions that are the customer's and the customer's beneficial owner's main places of business; and
- The jurisdictions to which the customer and the customer's beneficial owner have relevant personal links.

Product, service or transaction risk variables

- The purpose of an account or relationship;
- The regularity or duration of the business relationship;
- The level of assets to be deposited by a customer or the size of transactions undertaken;
- The level of transparency, or opaqueness, the product, service or transaction affords;
- The complexity of the product, service or transaction; and
- The value or size of the product, service or transaction.

Delivery channel risk variables

- The extent to which the business relationship is conducted on a non-face-to-face basis; and
- The presence of any introducers or intermediaries that the customer might use and the nature of their relationship with the customer.

Box 2 -- Lower risk factors (AMLR Annex II)

Customer risk factors

- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- Public administrations or enterprises; and
- Customers that are resident in geographical areas of lower risk as set out under Geographical risk factors.

Product, service, transaction or delivery channel risk factors

- Life insurance policies with low premiums;
- Insurance policies used for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes; and
- Products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership.

Geographical risk factors — registration, establishment, residence in:

- Member States;
- Third countries with effective AML/CFT systems;
- Third countries identified by credible sources as having a low level of corruption or other criminal activity; and
- Third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

Box 3 -- Higher risk factors (AMLR Annex III)

Customer risk factors

- the business relationship or occasional transaction is conducted in unusual circumstances;
- Customers that are resident in geographical areas of higher risk as set out under Geographical risk factors;
- Legal persons or legal arrangements that are personal asset-holding vehicles;
- Corporate entities that have nominee shareholders or shares in bearer form;
- Businesses that are cash-intensive;

- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
- The customer is a third country national who applies for residence rights in a Member State in exchange of any kind of investment, including capital transfers, purchase or renting of property, investment in government bonds, investment in corporate entities, donation or endowment of an activity contributing to the public good and contributions to the state budget;
- The customer is a legal entity or arrangement created or set up in a jurisdiction in which it has no real economic activity, substantial economic presence or apparent economic rationale; or
- The customer is directly or indirectly owned by one or several entities or arrangements as described in the point above.

Product, service, transaction or delivery channel risk factors

- Private banking;
- Products or transactions that might favour anonymity;
- Payment received from unknown or unassociated third parties;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products; or
- Transactions related to oil, arms, precious metals or stones, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

Geographical risk factors

- Third countries subject to increased monitoring or otherwise identified by the FATF for compliance weaknesses in their AML/CFT systems;
- Third countries identified by credible sources/acknowledged processes, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- Third countries identified by credible sources/acknowledged processes as having significant levels of corruption or other criminal activity;
- Third countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the UN;
- Third countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
- Third countries identified by credible sources or pursuant to acknowledged processes as enabling financial secrecy by:
    - posing barriers to the cooperation and exchange of information with other jurisdictions;
    - having strict corporate or banking secrecy laws which prevent institutions and their employees from providing customer information to competent authorities, including through fines and penalties;
    - having weak controls for the creation of legal entities or setting up of legal arrangements; or
    - not requiring beneficial ownership information to be recorded or held in a central database or register.

Third country branches and subsidiaries

If an obliged entity has a branch or subsidiary in a third country where the requirements are less strict than the AMLR, the branch or subsidiary must be brought up to the AMLR's standards.[26] If a third country's laws do not allow this, the obliged entity will have to take additional measures to deal with the risk of money laundering and terrorist financing. It must also inform its home Member State supervisor.

If the home Member State supervisor does not consider this adequate, it can prevent or terminate new or existing relationships and business transactions involving the branch or subsidiary or close the third country operation.[27]

Outsourcing

Outsourcing is still permitted, but only for some, not all, AML/CFT functions. Where outsourcing is allowed, the obliged entity is still fully liable for the proper discharge of the outsourced functions and the outsourced service provider must comply with the obliged entity's relevant policies. There can be no new barriers to monitoring and supervision as a result of an outsourcing. The obliged entity must also demonstrate that (i) it understands the activities carried out by the service provider it chooses, (ii) the service provider is properly qualified to carry them out, and (iii) there is a written agreement on the tasks to be outsourced and the way in which they are monitored.

The tasks that cannot be outsourced are:

1. The proposal and approval of the obliged entity's business-wide risk assessment;
2. Approval of the obliged entity's internal policies, procedures and controls;
3. Deciding the risk profile to be attributed to the customer;
4. The decision to enter into a business relationship or carry out an occasional transaction with a client;
5. Reporting to FIUs of suspicious activities or threshold-based reports, except where such activities are outsourced to another obliged entity belonging to the same group and established in the same Member State; and
6. Approving the criteria for detecting suspicious or unusual transactions and activities.[28]

Limited exemption for some AIFs and UCITS

There is an outsourcing exemption for AIFs or UCITS if they (i) have no legal personality or (ii) have only a board of directors which has delegated processing subscriptions and

[26] *See* AMLR Article 17(1) (Branches and subsidiaries in third countries).
[27] *See* AMLR Article 17(2) (Branches and subsidiaries in third countries).
[28] *See* AMLR Article 18(3)(a) to (f) (Outsourcing).

collection of "funds"[29] from investors to another entity. In these cases, they can outsource tasks 3 to 5 from the list of matters that otherwise cannot be outsourced, but only if prior notification has been given to and approval received from the supervisor. For the outsourcing to be permitted, the service provider must have resources, experience and knowledge on preventing money laundering and terrorist financing and understand the activities or transactions carried out by the AIF or UCITS.

Other exemptions

The exemption for small transactions that are not core to an entity's regular business and occasional remains broadly unchanged.[30]

Outsourcing to third countries

Where any functions (not just the ones that cannot normally be outsourced) are outsourced to service providers in third countries, extra requirements apply. This can only be done if:

- The tasks are only outsourced to a service provider in the same group as the obliged entity; and
- The group applies AML/CFT policies and procedures, CDD measures and rules on record keeping that are fully in compliance with the AMLR or equivalent third country rules and compliance with these requirements is supervised at a group level by the home Member State supervisor.[31]

Compliance function

The AML Package clarifies and gives new details on the obliged entities' compliance functions, who staffs them and how those members of staff should be vetted and protected against pressure on how they discharge their functions.[32]

AMLR contains an explicit requirement to have a dedicated compliance function. An obliged entity must have a member of its management board responsible for complying with both the AMLR and, where relevant, the new Transfer of Funds Regulation which applies to some crypto assets.[33] This will require training for the member of the management board as well as staff (see below).

Compliance managers will need to include the new requirements for business-wide risk assessments when they make and update their own policies and ensure the management body is aware of them when approval is requested.

They continue to have to:

---

29 This is referencing "funds" as defined in Article 4, point (25), of Directive (EU) 2015/2366 (the Payments Services Directive) ("'funds' means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC [(the e-money directive) which 'lays down the rules for the taking up, the pursuit and the prudential supervision of the business of electronic money institutions.')].").

30 *See* AMLR Article 6(1) (Exemptions for certain financial activities).

31 *See* AMLR Article 18(6) (Outsourcing).

32 *See* AMLR Article 11 (Compliance functions).

33 *See* the Travel Rule, *supra* note 19.

- Be sure the internal policies, procedures and controls are consistent with the risks the obliged entity is exposed to and that they are implemented;
- Make sure sufficient human and material resources are in place; and
- Be responsible for receiving information on any significant or material weaknesses in the policies, procedures and controls.

This obligation also applies to the obliged entity's management body. The compliance manager must also report to the management body on how effective the obliged entity's internal policies, procedures and controls are at least annually.

Obliged entities also must have a compliance officer with "sufficient hierarchical standing" to be able to carry out day-to-day AML/CFT duties as well as for targeted financial sanctions, submitting suspicious transactions and being a contact point for competent authorities.

In line with the principle of proportionality, the compliance officer can also carry out the functions within the obliged entity provided it is justified by its size and low risk or it is part of a group where someone else performs that function.

To remove a compliance officer prior notice has to be given to the obliged entity's management body. The obliged entity also has to tell its supervisor and explain if the removal relates to work subject to the rules in the Package. The compliance officer has the right to give information to the supervisor about his or her removal.[34]

As well as ensuring the compliance officer has sufficient resources to carry out the functions and be able to report direct to the board, the obliged entity "shall take measures to ensure that the compliance officer is protected against retaliation, discrimination and any other unfair treatment, and that decisions of the compliance officer are not undermined or unduly influenced by commercial interests of the obliged entity."[35]

Staff and staff training

The AML Package replaces the previously quite high-level requirements on staffing and staff integrity with a more detailed set of requirements.[36] Obliged entities will need to review the new requirements to ensure they will continue to be comply with them.

These new requirements include obligations to make sure relevant staff, agents and distributors know about the requirements and obligations of the AMLR. Part of this will involve ongoing training on how to spot money laundering and terrorist financing activities and what to do about it. The training needs to be appropriate to their functions or activities and appropriate to the risks to which the obliged entity is exposed.

Before a staff member is appointed to the compliance function, an obliged entity also must be sure the individual has the skills, knowledge and expertise to carry out tasks effectively and be of good repute, honesty and integrity. There must be conflicts of

[34] *See* AMLR Article 11(2), (Compliance function).
[35] *See* AMLR Article 11(4) (Compliance functions).
[36] *See* AMLR Article 13 (Integrity of employees).

interest procedures in place. These requirements also apply to the appointment of agents and distributors.

Beneficial Ownership

The definition of and threshold for who is a beneficial owner is maintained but there are new monitoring requirements.

3

3.1 Identification of beneficial owners

While what constitutes beneficial ownership and the thresholds for when it takes effect have been maintained, the AML Package expands the requirements to both obliged entities and national supervisors with respect to the identification, ongoing monitoring and reporting of beneficial owners. While there are some new factors, such as for collective investment undertakings (discussed below in Box 5), many changes are minor adjustments in wording but will still need to be reviewed in detail against current practices.

The concept of beneficial ownership has two parts. First, a beneficial owner of a legal entity is a natural person who directly or indirectly has either directly or indirectly an ownership interest, or who controls, directly or indirectly, the corporate or other legal entity by an ownership interest or other means. Second, the direct or indirect interest amounts to 25% or more of the shares, voting rights or other methods of ownership interest.[37] The beneficial ownership threshold can be set at 15% if it is justified by a national risk assessment.[38] The 25% figure is in line with international norms.

Box 4 -- Beneficial ownership of collective investment undertakings

This main definition is modified for AIFs and UCITS.[39] For AIFs and UCITS, beneficial owners are natural persons meeting one or more of the following conditions:

- They hold directly or indirectly 25% or more of the units held in the collective investment undertaking;
- They have the ability to define or influence the investment policy of the collective investment undertaking;
- They control the activities of the collective investment undertaking through other means.

There are new and more detailed requirements for identifying the different forms beneficial owners can use to control assets or entities, for example via ownership interest, control and the use of other legal arrangements such as trusts.[40]

3.2 Minimum data requirements for beneficial owners

At the least, obliged entities must collect:

- All names and surnames, place and full date of birth, residential address, country of residence and nationality or nationalities of the beneficial owner, numbers for identity documents, such as a passport or national identity document, and, where it exists, unique personal identification number assigned to the person by his or her country of usual residence, with a description of the source of that number;

37 *See* AMLR Article 51 (Identification of beneficial owners for legal entities) and Article 52 (Beneficial ownership through ownership interest).

38 *See* AMLR Article 52(2) (Beneficial ownership through ownership interest)

39 See AMLR Article 61 (Identification of beneficial owners of collective investment undertakings).

40 *See, e.g.,* AMLR Article 52 (Beneficial ownership through ownership interest), Article 53 (Beneficial ownership through control), Article 54 (Coexistence of ownership interest and control in the ownership structure) and Article 55 (Ownership structures involving legal arrangements or similar legal entities).

- The nature and extent of the beneficial interest held in the legal entity or legal arrangement, whether through ownership interest or control via other means and the date from when the beneficial interest is held;
- Information on the legal entity of which the natural person is the beneficial owner or, in the case of legal arrangements of which the natural person is the beneficial owner, basic information on the legal arrangement; and
- Where the ownership and control structure has more than one legal entity or legal arrangement, a description of the structure, including names and, where it exists, identification numbers of the individual legal entities or legal arrangements that are part of that structure, and a description of the relationships between them, including the share of the interest held.[41]

Where it is not possible to confirm the identity of a beneficial owner, it needs to be documented and the home Member State supervisors informed. Unless it is for a low risk activity or action, the information has to be obtained before entering into the business arrangement.

Box 5 -- AIFs and UCITS with no legal personality

Where an AIF or UCITS has no legal personality, the AIFM or UCITS management company is responsible for collecting and reporting beneficial ownership information.

AMLR Recital 23 clarifies that this should not lead to the fund and fund manager doing the same overlapping task twice, stating that:

> "[a]s both funds and fund managers fall within the scope of AML/CFT requirements, it is appropriate to clarify that a duplication of efforts should be avoided. To that end, the AML/CFT measures taken at the level of the fund and at the level of its manager should not be the same, but should reflect the allocation of tasks between the fund and its manager."

3.3 Monitoring beneficial owner activity

The requirements for monitoring customer behaviour and transactions have also been increased and more detailed rules on how this is done have been introduced.

Obliged entities must now assure themselves that they understand the purpose and intended nature of a of a business relationship or occasional transaction before entering into it. To do this they may need to get information on:

- The purpose and economic rationale;
- The estimated amount of the expected activities;
- The source of funds;
- The destination of funds: and

[41] *See* AMLR Article 22 (Identification and verification of the identity of customers and beneficial owners).

- The customer's business activity or occupation.[42]

There must be on-going monitoring by obliged entities to make sure customers' risk profiles and business activities remain consistent over time. This also applies to activities within a group.[43] For higher risk customers their documents, data and information must be checked every year. For all other customers they must be checked every five years.[44]

There are also the more detailed suspicious transaction reporting requirements described in **Section 5** of this summary. The reporting, data sharing and personal data obligations for obliged entities are also discussed in detail in that section.

[42] *See* AMLR Article 25 (Identification of the purpose and intended nature of a business relationship or occasional transaction).
[43] *See* Article 26(1) (Ongoing monitoring of the business relationship and monitoring of transactions performed by customers).
[44] *See* Article 26(2) (Ongoing monitoring of the business relationship and monitoring of transactions performed by customers).

Due Diligence

The existing basic due diligence requirements are broadly unchanged, although there are some changes to thresholds and amendments. There is greater detail on simplified and enhanced due diligence requirements.

4

4.1 CDD measures

The AML Package has amended and added to the requirements for CDD checks to screen for people or entities who might pose a money laundering or terrorist financing risk. The usual CDD checks obliged entities are expected undertake remain broadly unchanged but there are new requirements for crypto-assets and services. Other adjustments include more detail on when the high-level triggers for simplified CDD checks are justified, a change to the deadline for reporting them and more requirements for enhanced CDD. These changes are discussed further below.

The factors obliged entities must use all these due diligence measures using their business wide risk assessments and the risk factors (Boxes 2 and 3) are set out in **Section 2.2** of this summary.

If it is not possible to comply with the CDD requirements, the obliged entity must not establish a business relationship with, or carry out a transaction for, the customer.[45] It should also consider reporting a suspicious transaction to its home Member State FIU.

Legal entities seeking to be customers of obliged entities must provide information on their beneficial ownership if they are undergoing CDD.[46] This also applies to legal entities created in third countries.[47]

Occasional transactions threshold

There is a significant change to when CDD measures should be put in place for occasional transactions.[48] The previous threshold of €15,000 for carrying out an occasional transaction has been reduced to €10,000,[49] for transactions carried out in a single operation or through linked transactions. This threshold can be lower for certain transactions, such as for transactions with CASPs, at €1,000.

Simplified due diligence

Where it is justified using the risk factors in Boxes 1 and 2, obliged entities can apply simplified due diligence checks.[50] This allows:

- Verification of the identity of the customer and the beneficial owner after the establishment of the business relationship, but no later than 60 days from the relationship being established;
- Reducing the frequency of customer identification updates;
- A reduction in the amount of information collected to identify the purpose and intended nature of the business relationship or occasional transaction or inferring it from the type of transactions or business relationship established; and

45 *See* AMLR Article 21 (Inability to comply with the requirement to apply customer due diligence measures).
46 *See* AMLR Article 63 (Obligations of legal entities).
47 *See* AMLR Article 67 (Foreign legal entities and foreign legal arrangements).
48 *See* AMLR Article 19(1)(b) and (3) (Application of customer due diligence measures).
49 Or the equivalent in national currency.
50 *See* AMLR Article 33 (Simplified due diligence measures).

- Reducing the frequency or degree of scrutiny of transactions carried out by the customer.

The AMLA has the power to make further simplifications available.[51]

Enhanced due diligence

There is a new requirement that if a business relationship identified as higher risk involves assets of at least €5 million or personalised services where the financial or other assets are at least €50 million then further due diligence measures have to be applied:

- Specific measures including procedures to mitigate risks associated with personalised services and products offered to that customer;
- Obtaining additional information on the customer's source of funds; and

  Preventing and managing conflicts of interest between the customer and senior management or employees of the obliged entity that undertake tasks related to that obliged entity's compliance in relation to that customer.[52]

Box 6: Anonymity and anonymous instruments

New bearer shares continue to be prohibited, but where they exist, they must now be converted into registered shares, although there are limited exceptions.[53]

Financial institutions and CASPs now cannot keep anonymous accounts or allow anonymity to be created via "obfuscation of transactions" or coins. Before any existing instruments or accounts are used they must go through an appropriate due diligence process.

CASPs and self-hosted addresses

As well as having internal policies and procedures for their AML/CFT obligations in place, crypto-asset transactions to or from self-hosted addresses must:

- Take risk-based measures to identify, and verify the identity of, the originator or beneficiary of a transfer made from or to a self-hosted address or beneficial owner of such originator or beneficiary, including through reliance on third parties;
- Require additional information on the origin and destination of the crypto assets;
- Do enhanced ongoing monitoring of transactions with a self-hosted address;
- Use any other measure to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation and evasion of targeted financial sanctions.

The AMLA will develop guidelines the criteria for identifying the originator or beneficial owner of such transactions and for whether a self-hosted address is owned or controlled by a customer.[54]

---

51 *See* AMLR Article 28 (RTS on the information necessary for the performance of CDD).
52 *See* AMLR Article 34(5) (Scope of application of enhanced due diligence measures).
53 *See* AMLR Article 79(3) (Anonymous accounts and bearer shares and bearer share warrants).
54 *See* AMLR Article 40 (Measures to mitigate risks in relation to transactions with a self-hosted address).

4.2 Reliance on CDD performed by other obliged entities

Under the AML Package, it remains possible to rely on CDD that has been carried out by other obliged entities including those in third countries.[55] The ultimate responsibility for compliance remains with the obliged entity making use of another's work. Again, obliged entities must do this with reference to the details in Boxes 1 to 3.

The other obliged entity must apply the EU CDD rules, or equivalent rules if it is in a third country, and comply with EU AML/CFT standards, or in a way that is consistent with them.

4.3 PEPs

Although there are some adjustments to the definition of PEPs introduced by the AML Package, overall there are relatively few changes.[56]

The extra details to take account of are:

- Further detail on what constitutes a PEP in a Member State who is a member of a governing body of a political party;
- For members of the administrative, management or supervisory bodies of State-owned enterprises, references to the EU Accounting Directive;[57]
- More detail on levels of seniority in international organisations;
- The addition of civil unions or registered partnerships and the children of them;
- A rewording of the definition of "senior management";
- Further detail on "business relations";
- A new definition of "linked transactions": and
- A new definition of "third country", which is not in the EU but has its own AML/CFT regime.

4.4 Jurisdictional risk assessments

Obliged entities must consider the risk assessments that have to be carried out by EEA jurisdictions' relevant supervisors and the AMLA for the EU as a whole[58] and by the European Commission for third countries.[59]

---

55 *See* AMLR Article 48 (General provisions relating to reliance on other obliged entities); Article 49 (Process of reliance on another obliged entity); and Article 50 (Guidelines on reliance on other obliged entities).

56 *See* AMLR Article 2 (Definitions), sub-paragraphs (34) to (36).

57 *See* EU Directive 2013/34, available at https://eur-lex.europa.eu/eli/dir/2013/34/oj, at Articles 3(3), 3(4), 3(6), 3(7) and 22.

58 *See* AMLD6 Article 7 (Risk assessment at Union level) and Article 8 (National risk assessment).

59 *See* AMLR Article 29 (Identification of third countries with significant strategic deficiencies in their national AML/CFT regimes); Article 30 (Identification of third countries with compliance weaknesses in their national AML/CFT regimes); Article 31 (Identification of third countries posing a specific and serious threat to the Union's financial system); and Article 35 (Countermeasures to mitigate money laundering and terrorist financing threats from outside the Union).

The European Commission can require both obliged entities and national supervisors to have extra requirements based on these assessments.

If this is the case, obliged entities have to:

- Apply additional elements of enhanced due diligence;
- Have enhanced reporting mechanisms or systematic reporting of financial transactions; and
- Limit business relationships or transactions with natural persons or legal entities from those third countries.

Member States must require:

- Increased supervisory examination or increased external audit requirements for branches and subsidiaries of obliged entities located in the third country concerned;
- Increased external audit requirements for financial groups for any of their branches and subsidiaries located in the third country concerned; and
- Credit institutions and financial institutions to review and amend, or if necessary terminate, correspondent relationships with respondent institutions in the third country concerned.

Member States can also refuse to allow subsidiaries or branches or representative offices of obliged entities from those countries and/or prohibit obliged entities from establishing branches or representative offices in the third countries concerned.

Reporting and Information Sharing

The AML Package makes changes in how data is reported and shared. This goes wider than obliged entity reporting to national supervisors and FIUs. It creates a central database run by the AMLA and introduces formal cooperation requirements between AMLA and the FIUs and national supervisors.

5

5.1 Beneficial ownership reporting obligations

All obliged entities must submit the minimum beneficial ownership details discussed briefly in **Section 3.1** of this summary. This information has to be reported to their home Member State's central register "without delay" and kept up to date with any changes notified within 28 calendar days.[60] Internal systems need to be in place to facilitate this. This includes informing them of circumstances when no beneficial owner can be identified. Where an error or discrepancy is identified, this must be corrected within 14 days and if this is not possible the fact has to be reported to the relevant central register.

It is not yet clear how the reporting requirements will apply to non-EU AIFs or non-EU AIFMs which are in scope of the AML Package.

5.2 Suspicious activity reporting

Where there is a suspicion that a transaction could be for money laundering or terrorist financing, the obliged entity must report it to their FIU. This is regardless of the amount of the transaction. If the FIU requests further information, it must be provided within five days. Where justified by the circumstances, FIUs can request further detail to be given to them within 24 hours.[61] The obliged entity's compliance officer is responsible for suspicious activity reporting.

Grounds for suspicions are:

- The characteristics of the customer and their counterparts;
- The size and nature of the transaction or activity or the methods and patterns relating to it;
- The link between several transactions or activities, the origin, destination or use of funds; or
- Any other factors the obliged entity is aware of. These include due diligence findings on the consistency of the transaction or activity and the risk profile of the client.

If suspicions are raised where several obliged entities are sharing information, they can appoint one to inform the FIU. It must also say who the other members of the information-sharing partnership are. Where obliged entities are established in more than one Member State the FIUs of all those Member States are liable.

Provided the disclosure of information to the FIU is made in good faith, then it will not amount to a breach of contract or impose a liability on the obliged entity or its staff. This applies: "even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred."[62]

This information must not be shared with the customer subject to the report. Groups and information sharing partnerships can share this information internally provided procedures are in place to meet the overall requirement not to tell the customer.

60 *See* AMLR Article 69 (Reporting of suspicions).
61 *See* AMLR Article 69 (1)(b) (Reporting of suspicions).
62 *See* AMLR Article 72 (Disclosure to FIU).

5.3 Central registers and access to them

All member States must have a central register for beneficial ownership information.[63] Obliged entities may be given access to these national registers to verify beneficial ownership data and identify discrepancies in the data they have gathered.[64]

Supervisory authorities must set up secure systems to allow the data to be shared with other EEA supervisors and the AMLA.

A number of other interested parties, such as third country counterparts to EU supervisors, civil society organisations and journalists, can also gain access to central databases,[65] subject to conditions.[66] Individual supervisors can decide the access fee which must not exceed the cost of giving it. The European Commission has to create uniform templates for access purposes.[67]

5.4 Record retention

Specific documents and information must be kept for five years from the date a business relationship ends, from the end of an occasional transaction or when an obliged entity refuses to enter into a business arrangement with a potential customer.[68] These records must be unredacted and include:

- The information used to carry out customer diligence;
- The assessment and its results. If it leads to a suspicious transaction report, a copy sent to the FIU;
- Supporting evidence and records of transactions; and
- Where there is an information sharing arrangement in place, records of when information sharing took place.

At the end of five years records must be deleted in compliance with the EU General Data Protection Regulation.[69] However, supervisors can order records to be kept for up to an extra five years if they are needed for further AML/CFT purposes.[70]

63 *See* AMLD6 Article 10 (Central beneficial ownership registers).
64 See AMLD6 Article 11(4), (General rules regarding access to beneficial ownership registers by competent authorities, self-regulatory bodies and obliged entities).
65 *See* AMLD6 Article 12(2) (Specific access rules to beneficial ownership registers for persons with legitimate interest) for the full list.
66 *See* AMLD6 Article 13 (Procedure for the verification and mutual recognition of a legitimate interest to access beneficial ownership interest) and AMLD6 Article 15 (Exemptions to the access rules to beneficial ownership registers).
67 *See* AMLD6 Article 14(1) (Templates and procedures).
68 *See* AMLR Article 77(3) (Record retention).
69 *See* Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
70 *See* AMLR Article 77(4) (Record retention).

Supervision and the AMLA

The European supervisory architecture for AML/CFT is changed by the AML Package. Greater uniformity in the way in which the rules are complied with and supervised is one of the AML Package's key aims. The AMLA has wider powers and responsibilities than those currently available to the EBA. As the new European AML supervisory authority, AMLA has a role in coordination, data collection and supervision of "selected obliged entities".

6

6.1 The new supervisory structure

The AMLA will sit above the national supervisory authorities and FIUs already in place in Member States. It does not replace the current structure; it adds to it. The AMLA will coordinate supervision and be responsible for many of the more detailed rules, the "implementing measures" needed to fill in the detail needed for different parts of the AML Package. It will also run a new Union-wide beneficial ownership database and supervise selected obliged entities.

FIUs

All countries, not just those in the EEA, should have in place an FIU which meets the FATF's global standards.[71] They are different from national supervisory authorities, although there is nothing to prevent an FIU being part of one.

An FIU's core functions are:

- Receiving and analysing (i) suspicious transaction reports, and (ii) other information relevant to money laundering, associated predicate offences and terrorist financing; and
- Disseminating the results of its analyses.[72]

FIUs already work with their relevant national financial and non-financial supervisors. The AML Package extends that cooperation to the AMLA.

National supervisory authorities

Member States must have in place a body to supervise and enforce the AML/CFT rules.[73] That national supervisor must cooperate with other Member State national supervisors individually, in supervisory colleges and with the AMLA. Supervision should be risk-based and proportionate.

National supervisors must also give obliged entities in their jurisdictions information on the European Commission's EU-wide and third country assessments and the actions deemed appropriate for those jurisdictions as well as their own risk assessments and all relevant guidance. National supervisors and the AMLA must also have a central contact point.

AMLA duties and direct supervision

Expected to begin its activities in mid-2025, AMLA is supposed to have its full complement of 430 staff in place by 2027 and begin the direct supervision of selected obliged entities, described in relevant part in **Section 2.1** of this summary, in 2028. AMLA is also empowered to conduct on-site inspections of selected obliged entities. It

71 *See* AMLD6 Article 19(1) (Establishment of the FIU) and FATF Recommendations, *supra* note 1, at Recommendation 29.
72 *See* AMLD6 Article 19(3)(a) and (b) (Establishment of the FIU).
73 *See* AMLD6 Article 37 (Powers and resources of national supervisors).

can, in certain circumstances, take over supervision of non-selected obliged entities from national authorities.[74]

The AMLA must set up a central database which will detail each Member State's supervisory arrangements, details on their obliged entities and any supervisory activity.[75] The supervisory authorities must also send their national risk assessments to AMLA.

[74] *See* AMLAR Article 34 (Action in cases of systematic failures of supervision).
[75] *See* AMLAR Article 11 (Central AML/CFT database).

Annex I: Implementing Measures

AMLR, AMLD6 and AMLAR each contain a variety of empowerments to make guidance, delegated acts and regulatory technical standards. Below is a list of identifying these measures by source and date they are due.

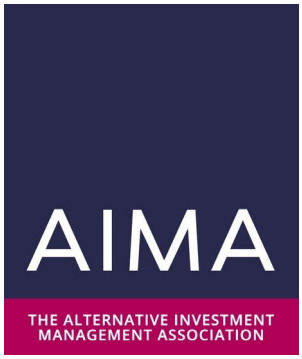
AMLR	Article 68(1) Penalties	10 January 2025
AMLD6	Article 10(6): Central beneficial ownership registers	10 July 2025
AMLAR	Article 11(6): Central AML/CFT database	27 December 2025
AMLAR	Article 12(7): Assessment of credit institutions and financial institutions for the purposes of selection for direct supervision	1 January 2026
	Article 15(3): Cooperation within the AML/CFT supervisory system for the purposes of direct supervision	
AMLAR	Article 41(2): Reporting and transmission of the results of joint analyses	27 June 2026
AMLR	Article 9(4): Scope of internal policies, procedures and controls	10 July 2026
	Article 10(4): Business-wide risk assessment	
	Article 16(4): Group-wide requirements	
	Article 17(3) and (4): Branches and subsidiaries in third countries	
	Article 19(9) Application of customer due diligence measures	
	Article 20(3): Customer due diligence measures	
	Article 26(5) Ongoing monitoring of the business relationship and monitoring of transactions performed by customers	
	Article 28(1): RTS on the information necessary for the performance of customer due diligence	
	Article 68(2): Penalties	
	Article 69(3): Reporting of suspicions	
	Article 81(1): Cooperation between FIUs and the EPPO	
AMLD6	Article 31(2) and (3): Exchange of information between FIUs	10 July 2026
	Article 40(2): Risk-based supervision	
	Article 41(2): Central contact points	
	Article 46(4): Provisions related to cooperation in the context of group supervision	

	Article 49(14): AML/CFT supervisory colleges in the financial sector	
	Article 50(13) AML/CFT supervisory colleges in the non-financial sector	
	Article 53(10): General provisions	
	Article 53(11) General provisions	
AMLD6	Article 11(5): General rules regarding access to beneficial ownership registers by competent authorities, self-regulatory bodies and obliged entities	10 October 2026
AMLAR	Article 27(7): Procedural rules for taking supervisory measures and imposing pecuniary sanctions and periodic penalty payments	1 January 2027
	Article 77(6): Fees levied on selected and non-selected obliged entities	
AMLR	Article 18(8): Outsourcing	10 July 2027
	Article 21(4): Inability to comply with the requirement to apply customer due diligence measures	
	Article 32(1): Guidelines on money laundering and terrorist financing risks, trends and methods	
	Article 34(5): Scope of application of enhanced due diligence measures	
	Article 37(3): Specific enhanced due diligence measures for cross-border correspondent relationships for crypto-asset service providers	
	Article 40(2): Measures to mitigate risks in relation to transactions with a self-hosted address	
	Article 42(2): Specific provisions regarding politically exposed persons	
	Article 50: Guidelines on reliance on other obliged entities	
	Article 69(5): Reporting of suspicions	
AMLR	Article 56: Notifications	10 October 2027
	Article 57(3): Identification of beneficial owners for legal entities similar to express trusts	
AMLD6	Article 53(5) General provisions	10 October 2027
AMLD6	Article 3(8) Identification of exposed sectors at national level	10 July 2028
	Article 5(5) Requirements relating to the granting of residence rights in exchange for investment	
	Article 7(2) Risk assessment at Union level	

	Article 10(7): Central beneficial ownership registers	
	Article 17(2) Implementing acts for the interconnection of registers	
	Article 19(10): Establishment of the FIU	
	Article 28(1): Feedback by FIUs	
	Article 31(4) Exchange of information between FIUs	
	Article 31(8): Exchange of information by FIUs	
	Article 34(3) Consent to further dissemination of information exchanged between FIUs	
	Article 40(3): Risk-based supervision	
AMLR	Article 52(2): Beneficial ownership through ownership interest	10 July 2029
AMLD6	Article 6(8): Checks on the senior management and beneficial ownership of certain obliged entities	10 July 2029
	Article 9(4): Statistics	
	Article 16(6) Bank account registers and electronic data retrieval systems	
	Article 31(9) Exchange of information between FIUs	
	Article 34(4) Consent to further dissemination of information exchanged between FIUs	
	Article 50(14): AML/CFT supervisory colleges in the financial sector	
	Article 51(4): Cooperation with supervisors in third countries	
	Article 64(6): Cooperation in relation to credit institutions or financial institutions	
	Article 69: AML/CFT cooperation guidelines	
AMLD6	Article 5(7) Requirements relating to the granting of residence rights in exchange for investment	10 July 2030
	Article 7(5): Risk assessment at Union level	
	Article 7(7) Risk assessment at Union level	
	Article 9(6) Statistics	
AMLAR	Article 102(1): Evaluation and review	31 December 2030

AMLD6	Article 10(21): Central beneficial ownership registers	10 July 2031
AMLD6	Article 18(6) Single access point to real estate information	10 July 2032
AMLR	Article 16(5): Group-wide requirements	No date specified
	Article 29(2) Identification of third countries with significant strategic deficiencies in their national AML/CFT regimes	
	Article 30(2): Identification of third countries with compliance weaknesses in their national AML/CFT regimes	
	Article 31(9): Identification of third countries posing a specific and serious threat to the Union's financial system	
	Article 34(7): Scope of application of enhanced due diligence measure	
	Article 43(5): List of prominent public functions	
	Article 57(4): Identification of beneficial owners for legal entities similar to express trusts	
	Article 58(5): Identification of beneficial owners for express trusts and similar legal arrangements	
AMLD6	Article 9(5): Statistics	No date specified
	Article 14(1): Templates and procedures	
	Article 17(1): Implementing acts for the interconnection of registers	
AMLAR	Article 6(4): Powers of the Authority	No date specified
	Article 8(3) AML/CFT supervisory methodology	
	Article 16(6) Joint supervisory teams	
	Article 30(1) Assessments of the state of supervisory convergence	
	Article 77(6): Fees levied on selected and non-selected obliged entities	

Appendix A: About AIMA



The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than $3 trillion in hedge fund and private credit assets.

AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry.

AIMA set up the Alternative Credit Council (ACC) to help firms focused on the private credit and direct lending space. The ACC currently represents over 250 members that manage over $1 trillion of private credit assets globally.

AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA's website, www.aima.org.