

SHUFTI • REGULATORY GUIDE

EU AMLR: The Complete EU Compliance Guide **for 2027**

Regulation (EU) 2024/1624 is final and in force. Most requirements apply from 10 July 2027. This guide walks the whole rulebook, and flags every draft AMLA standard separately.



Twenty-seven questions, answered against the text

I THE REGULATION

- 01 What is the EU AMLR?
- 02 Why was AMLR introduced?
- 03 How do AMLR, AMLD6, AMLA and TFR fit together?
- 04 What changes under AMLR, and what was already there?
- 05 When does AMLR apply?

III THE CUSTOMER LIFECYCLE

- 08 When is customer due diligence required?
- 09 What does AMLR customer due diligence include?
- 10 What are the KYC requirements for individuals?
- 11 What are the KYB requirements for businesses?
- 12 Can customers be onboarded remotely?
- 13 How does risk affect due diligence?
- 14 What screening does AMLR require?
- 15 What does ongoing monitoring involve?

V REPORTING, DATA AND LIMITS

- 19 When must suspicious activity be reported?
- 20 What must be reported on high-value goods?
- 21 When can AML information be shared?
- 22 How does AMLR interact with GDPR, AI and recordkeeping?
- 23 What anonymity and cash restrictions does AMLR introduce?

II SCOPE AND REACH

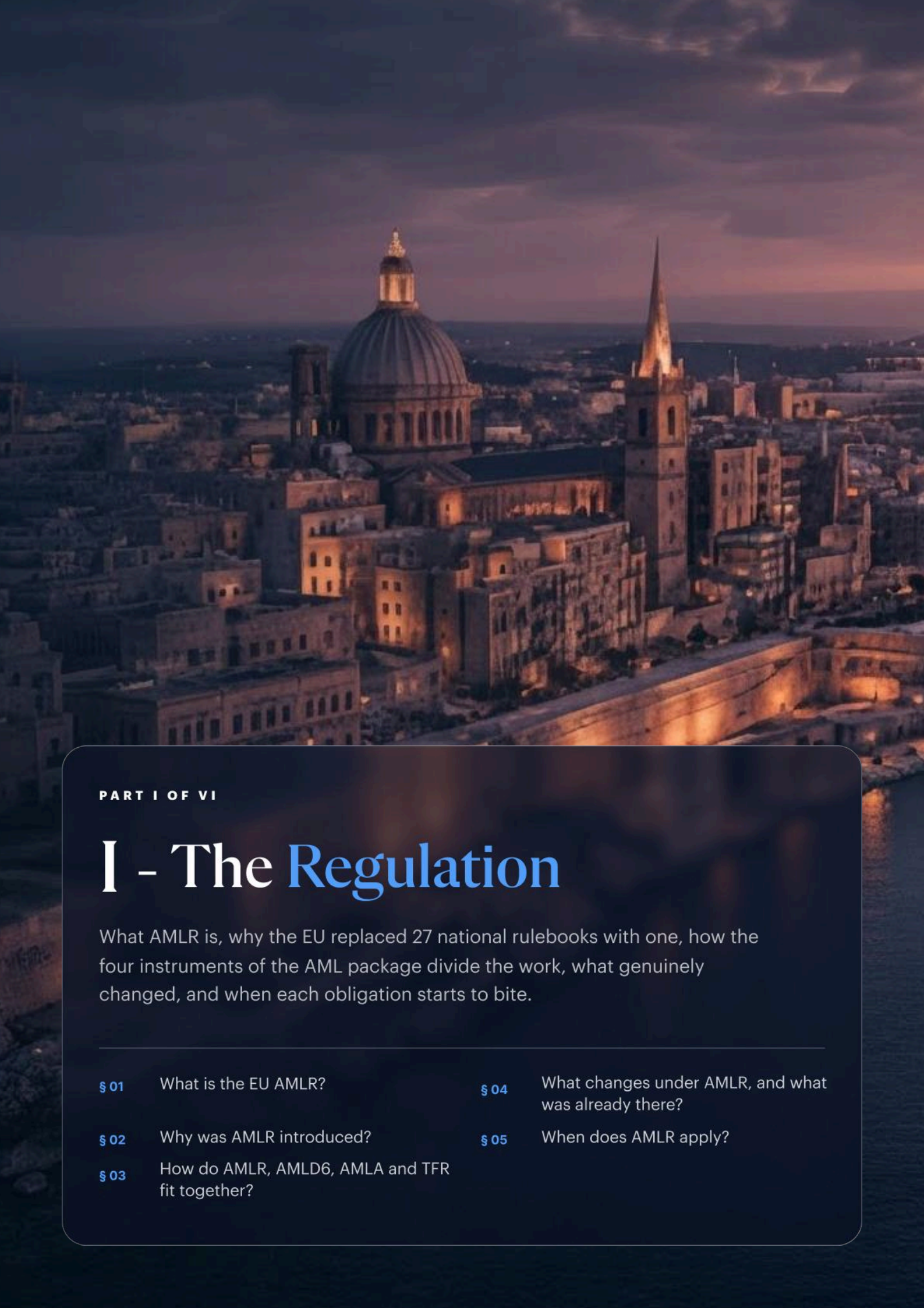
- 06 Who is subject to AMLR?
- 07 Does AMLR apply outside the EU?

IV OWNERSHIP AND HIGHER RISK

- 16 How is beneficial ownership determined?
- 17 Which situations require specific enhanced measures?
- 18 How does AMLR apply to crypto-assets?

VI GOVERNANCE, SUPERVISION AND CONSEQUENCES

- 24 What compliance framework does AMLR require?
- 25 Who supervises AMLR, and what does AMLA do?
- 26 What are the penalties for non-compliance?
- 27 How should organisations prepare for AMLR?
 - Where Shufti fits the AMLR lifecycle
- § Key legal and regulatory sources



PART I OF VI

I - The Regulation

What AMLR is, why the EU replaced 27 national rulebooks with one, how the four instruments of the AML package divide the work, what genuinely changed, and when each obligation starts to bite.

§ 01 What is the EU AMLR?

§ 02 Why was AMLR introduced?

§ 03 How do AMLR, AMLD6, AMLA and TFR fit together?

§ 04 What changes under AMLR, and what was already there?

§ 05 When does AMLR apply?

What is the EU AMLR?

The EU Anti-Money Laundering Regulation is the European Union's directly applicable rulebook for preventing money laundering and terrorist financing in the private sector.

It tells banks, financial institutions, crypto-asset businesses and a wide range of professional and non-financial firms how to assess risk, perform customer due diligence, identify beneficial owners, monitor relationships and report suspicious activity.

AMLR is the core of what the Commission calls the **EU AML single rulebook**. Where earlier EU law set common principles and left each Member State to write its own version, AMLR sets the obligations directly. National supervisors, financial intelligence units (FIUs), registers and a defined set of national options remain, but the requirements themselves no longer arrive through 27 separate transpositions.

Most provisions apply from **10 July 2027**.¹

Formal instrument	Regulation (EU) 2024/1624
Main application date	10 July 2027
Core purpose	Common EU AML/CFT requirements for obliged entities
Key lifecycle duties	CDD, KYC/KYB, ownership, screening, monitoring and reporting
Supervision	Primarily national, with AMLA coordination and selected direct supervision

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 90

Football is the one deferred sector, and it is narrower than it sounds

Two obliged-entity categories apply from **10 July 2029** rather than 2027: football agents, and professional football clubs.¹

Clubs are not in scope for everything they do. They are obliged entities only for four transaction types: transactions with an investor, with a sponsor, with football agents or other intermediaries, and for the purpose of a player's transfer.²

For example, a top-division club selling season tickets to supporters is not acting as an obliged entity. The same club paying commission to an agent on a player transfer is, because that payment falls inside two of the four listed types at once.

Member States may also exempt clubs entirely or partly, by two separate routes. Top-division clubs qualify where total annual turnover was under EUR 5,000,000 in each of the previous two calendar years. Clubs in any lower division qualify with no turnover threshold at all. Both routes require a documented Member State risk assessment and are optional, not automatic.³

KEY RULE

AMLR mandates measures that help businesses *prevent* money laundering. It does not replace the criminal law used to investigate and prosecute it.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 90 · Art 3(3)(n)-(o) ² Art 3(3)(o) ³ Art 5(1)-(3)

Why was AMLR introduced?

Earlier EU directives created common principles, but each Member State implemented them through different national laws: different definitions, thresholds, supervision and operational expectations. A group operating in eight Member States maintained eight interpretations of the same rule.

The Commission put numbers on that before it drafted AMLR. Its impact assessment for the AML package found most Member States setting the beneficial-ownership register threshold at 25%, with Latvia and Spain at 10%. It also found that national rules for calculating indirect ownership diverged far enough that the same corporate structure could produce different beneficial owners depending on which Member State assessed it.

AMLR centralises that into one rulebook, directly applicable in every EU country.

What harmonisation delivers

More harmonisation	Groups can design a stronger common EU baseline while retaining national overlays.
Expanded scope	Additional crypto, professional, high-value and other activities expressly covered.
More detailed CDD	Identity, ownership, purpose, risk and monitoring operate as one lifecycle.
Ownership transparency	Both ownership and control must be tested, and discrepancies addressed.
Lifecycle monitoring	Customer data and expected activity must remain current after onboarding.
Common restrictions	Limits on anonymous instruments and large professional cash payments.

What harmonisation does not remove

Direct applicability does not mean every national difference disappears. Member States retain responsibility for supervision, FIU processes, beneficial-ownership registers, sanctions machinery and the areas where AMLR permits national choices. A group operating in several Member States still needs a country overlay on top of the common baseline.

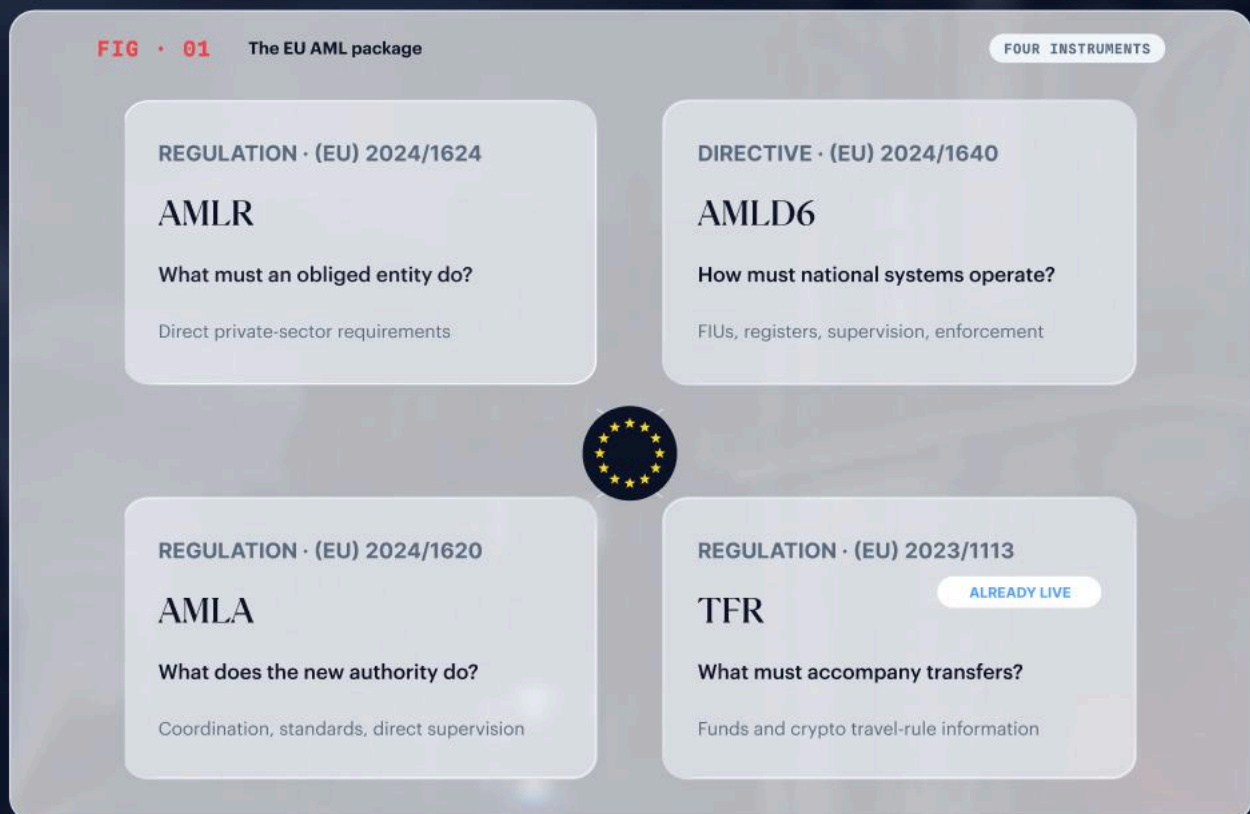
The overlay is thinner than it was. It is not gone.

What to carry forward

Treat the common baseline and the national overlay as two separate artefacts with two separate owners. The baseline follows AMLR and changes when AMLR changes. The overlay follows 27 supervisors, registers and FIU processes, and changes far more often. Firms that merged the two into a single country matrix under 5AMLD are the ones with the most rework ahead of them.

How do AMLR, AMLD6, AMLA and TFR fit together?

The EU AML package contains four instruments, and each answers a different question.



Two naming traps are worth avoiding. AMLR should not be called "AMLD6": the regulation carries the direct private-sector obligations, while the directive governs national machinery. And AMLD6 **is** the instrument informally called 6AMLD. It does not replace "6AMLD"; it repeals Directive (EU) 2015/849, the directive commonly called 4AMLD as amended by 5AMLD.

REGULATION AND DIRECTIVE, SIDE BY SIDE

	AMLR	AMLD6
Instrument type	Regulation, directly applicable	Directive, requires transposition
Binds	Obligated entities	Member States
Covers	CDD, KYC/KYB, beneficial ownership, screening, monitoring, reporting, cash and anonymity limits	Registers, FIUs, supervision, cooperation, penalties
Also called	The single rulebook	6AMLD
Applies or transposed by	10 July 2027	10 July 2027, with earlier deadlines for some articles
Replaces	National AML rulebooks built on Dir (EU) 2015/849	Dir (EU) 2015/849, repealed from 10 July 2027 ↓ AMLD6 Art 77

AMLD6 also transposes on a staggered schedule rather than a single date. General transposition is 10 July 2027, but Article 74 was due by 10 July 2025, the register-access provisions in Articles 11, 12, 13 and 15 by 10 July 2026, and the real-estate single access point by 10 July 2029.¹

The updated Transfer of Funds Regulation has applied since **30 December 2024**. Its payment and crypto travel-rule requirements are already live. They are not postponed until AMLR applies.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ AMLD6 Art 78(1)

What changes under AMLR, and what was already there?

Most AMLR coverage reads as though every requirement is new. For a firm already running a compliant 5AMLD programme, that is not useful. This section separates the genuinely new obligations from the ones that have simply moved instrument.

Start with the beneficial-ownership threshold, because it moved twice

PREVIOUS REGIME

"A shareholding of **25% plus one share** or an ownership interest of **more than 25%** in the customer held by a natural person shall be an indication of direct ownership."

Dir 2015/849 Art 3(6)(a)(i)

UNDER AMLR

"direct or indirect ownership of **25% or more** of the shares or voting rights or other ownership interest"

Art 52(1)

A natural person holding exactly 25.00% was not caught by the ownership indicator before. They are now.

For example, a customer company owned by four natural persons at exactly 25.00% each produced no beneficial owner under the ownership limb of the previous test. From 10 July 2027 it produces four.

KEY RULE

If any KYB rule engine, screening configuration or onboarding form you run carries a **> 25** test, it is wrong from 10 July 2027. It needs to be **>= 25**.

The second change sits in the same sentence. The old provision continued: "This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control." A Member State could unilaterally drop the threshold. Under AMLR it cannot. It may notify the Commission of higher-risk categories, and only the Commission sets a lower category-specific threshold, by delegated act, floored at 15% and in any case below 25%.¹

So the trigger got lower and the ability of 27 Member States to diverge on it was removed. If you built country-by-country UBO threshold logic to handle national variation, you are maintaining machinery AMLR is designed to make unnecessary.

The rest of the change map

Area	Previously	Under AMLR
Instrument	Directive, transposed 27 ways	Regulation, directly applicable ↓ Art 90
UBO threshold	More than 25%, or 25% plus one share	25% or more ↓ Art 52(1)
Lowering the threshold	Member State discretion	Commission delegated act only, floor 15% ↓ Art 52(2)
Ownership vs control	Control assessed, relationship to ownership left to national practice	Control tested "independently of and in parallel to" ownership, with no percentage floor ↓ Art 51 ↓ Art 53
Mixed chains	<i>Not addressed</i>	Art 54 replaces percentage arithmetic where ownership and control coexist across layers ↓ Art 54
No beneficial owner found	Identify senior managing officials, keep records	Statement, justification, full senior-managing-official details, and the term now defined ↓ Art 63(3)-(4)
Who holds BO information	Obligated entity investigates	Entities, owners, chain entities, trustees and nominees carry their own duties ↓ Arts 62-67
BO refresh	Risk-based, no EU deadline	28 calendar days from change, plus annual verification ↓ Art 62(2) ↓ Art 63(2)

Continued

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ [Art 52\(2\)](#)

THE CHANGE MAP, CONTINUED

Area	Previously	Under AMLR
Register discrepancies	Report, no EU day count	Without undue delay and in any case within 14 calendar days of detection ↳ Art 24(1)
Customer refresh	Risk-based, no EU cap	Hard maximum 1 year under enhanced due diligence, 5 years otherwise ↳ Art 26(2)
Deferred verification	Risk-based	Hard 60-day cap for qualifying low-risk relationships ↳ Art 33(1)(a)
High-net-worth EDD	General risk-based approach	Prescribed gate at EUR 5m handled and EUR 50m held ↳ Art 34(5)
Cash	National limits only	EU-wide EUR 10,000 ceiling on professional cash payments ↳ Art 80(1)
High-value goods	Traders as obliged entities	Plus threshold reports to the FIU at EUR 250,000 and EUR 7.5m ↳ Art 74
Crypto	Partial coverage	Crypto-asset service providers as full obliged entities, EUR 1,000 occasional threshold ↳ Art 19(3)
Crypto anonymity	<i>Not addressed</i>	Anonymous crypto accounts and anonymity-enhancing features prohibited ↳ Art 79(1)
Bearer shares	National treatment	Conversion or immobilisation by 10 July 2029, cancellation by 10 July 2030 ↳ Art 79(3)
New sectors	<i>Not covered</i>	Football agents and clubs, crowdfunding, investment migration, wider high-value trading ↳ Art 3(3)
Supervision	National only	National, plus AMLA direct supervision of a selected cohort from 2028 ↳ AML Reg Art 13

What did not change

The risk-based approach survives intact. So does the structure of customer due diligence, the tipping-off prohibition, the duty to report suspicion irrespective of amount, and the principle that simplified due diligence is a calibration rather than an exemption. If you have a working 5AMLD programme you are not starting again. You are tightening deadlines, widening scope, and rebuilding the ownership layer.

When does AMLR apply?

AMLR entered into force in 2024, but most operative requirements have a later application date. "In force" and "fully applicable" are not the same thing.¹

2024 - 2030

- 9 Jul 2024 ● AMLR enters into force, twentieth day after OJ publication of 19.6.2024
- 30 Dec 2024 ● TFR applies, travel rule already live
- 1 Jul 2025 ● AMLA Regulation applies, Authority stands up
- 10 Jul 2025 ● AMLD6 Art 74 transposition due
- 31 Dec 2025 ● Commission stewardship of AMLA ends
- 8 May 2026 ● Art 28 CDD RTS consultation closed, results pending
- 10 Jul 2026 ● AMLD6 register-access articles due
- 3 Sep 2026 ● Art 26(5) monitoring guidelines consultation closes
- 1 Jul 2027 ● AMLA first selection process commences
- 10 Jul 2027 ● **Most AMLR requirements apply**
- 2028 ● AMLA direct supervision begins
- 10 Jul 2029 ● Football provisions apply; bearer share conversion deadline; AMLD6 real-estate access point due
- 10 Jul 2030 ● Unconverted bearer shares cancelled

● AMLR ● AMLA / AMLD6 ● Key date

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 90

One date matters most: **10 July 2027**. Track final law, draft Level 2 measures (the technical standards and guidelines that sit beneath the Regulation), transitional guidance and national rules as four separate workstreams. They move at different speeds, and collapsing them into one plan is how a programme ends up waiting on a standard it did not need.¹

Level 2 status

AMLA's regulatory-instruments tracker lists the Article 28 CDD regulatory technical standard as draft. Its consultation closed on 8 May 2026 and results are pending. The Article 26(5) ongoing-monitoring consultation remains open until 3 September 2026. Existing EBA instruments identified by AMLA continue to apply until replacement measures take effect. Re-check this status before relying on any Level 2 detail.



PART II OF VI

II – Scope and Reach

Which businesses AMLR binds, which are covered only for defined activities, and how a non-EU organisation works out whether it has an EU nexus at all.

§ 06 Who is subject to AMLR?

§ 07 Does AMLR apply outside the EU?

Who is subject to AMLR?

AMLR applies to obliged entities. Scope can attach to an entire regulated business, or only to specified professional activities and transactions.¹

THE OBLIGED-ENTITY MAP

Sector	Who is covered	Scope note
Banks and credit	Banks, credit institutions	Whole business
Payments and fintech	Payment and e-money institutions, payment initiation and account information providers	Whole business
Investment and insurance	Investment firms, relevant life and investment insurers and intermediaries	Whole business
Crypto	In-scope crypto-asset service providers	Whole business. Authorisation and definitions sit in MiCA
Lawyers and notaries	Notaries, lawyers and other independent legal professionals	Only for defined activities and transactions
Accountants and tax	Auditors, external accountants, tax advisers	Only for defined activities
Trust and company services	Trust or company service providers	Whole business
Real estate	Estate agents and defined real-estate professionals	Activity-dependent. Both parties count as customers ↳ Art 19(6)(c)

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 3

THE OBLIGED-ENTITY MAP, CONTINUED

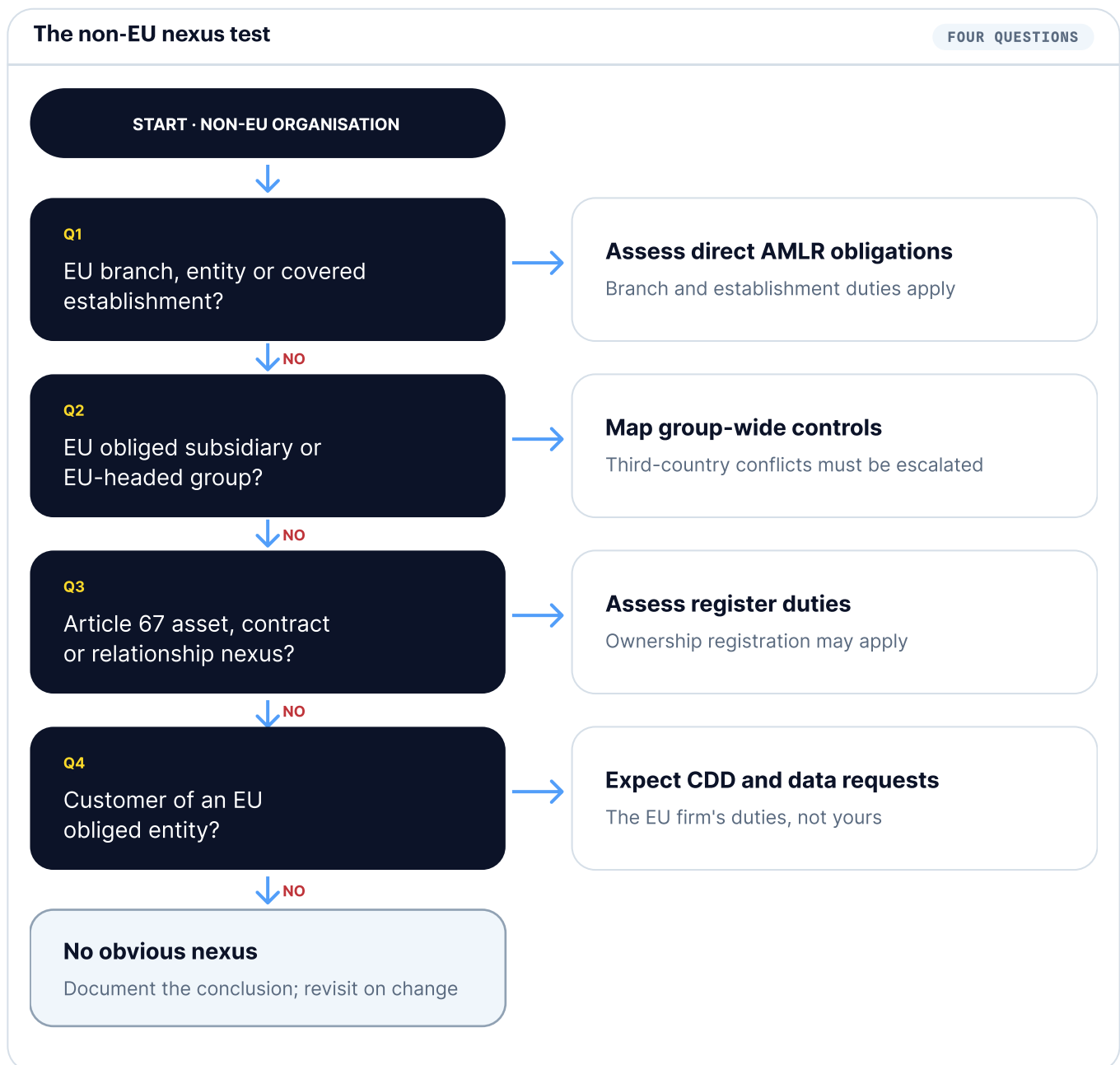
Sector	Who is covered	Scope note
Gambling	Providers of gambling services	Member States may exempt defined low-risk services ↓ Art 4
High-value and luxury goods	Traders in and intermediaries for precious metals and stones, jewellery, watches, luxury motor vehicles, aircraft and watercraft	Threshold and activity-dependent
Art and culture	Art-market participants, including intermediaries and those storing art in free zones	Threshold-dependent
Crowdfunding	Crowdfunding service providers and intermediaries	Whole business
Investment migration	Operators involved in residence-by-investment schemes	Activity-dependent
Holding companies	Certain non-financial mixed-activity holding companies	Structure-dependent
Football	Football agents; professional football clubs for four transaction types	From 10 July 2029. Member State exemptions available ↓ Art 5

Not every person working in a listed sector is automatically covered. For legal professionals, goods traders, property businesses and football organisations, the activity and transaction conditions are decisive. Member States may also add sectors or apply defined exemptions, so test the specific activity against the Regulation first and the national overlay second.

Confirm which entities, branches and activities are covered before designing controls. A scope error propagates through every downstream decision.

Does AMLR apply outside the EU?

AMLR binds the 27 Member States, with EEA relevance. It is not a universal worldwide regime. A non-EU organisation should look for a specific EU nexus rather than assume it is either fully in or fully out.



Does AMLR apply to UK businesses?

For a UK business the position is interpretive rather than a single article. The UK remains under the Money Laundering Regulations 2017. But EU subsidiaries and branches of UK groups are obliged entities in their own right, and AMLR's group-wide policy obligations reach EU-facing UK parents.¹

A UK firm asked by an EU counterparty for identity, ownership or source-of-funds information is usually seeing that counterparty's duties at work, which does not by itself make the UK firm an obliged entity.

Foreign entities can also acquire a direct register duty under Article 67, triggered by an EU business relationship, EU real estate, defined high-value goods purchases, or an EU public contract.²

Two questions, kept apart

"Are we an obliged entity?" and "do we have an AMLR-driven obligation?" have different answers. A non-EU firm with no EU establishment can still owe register information under Article 67, and can still be asked for evidence by every EU counterparty it deals with. Neither makes it an obliged entity. Record which of the two you concluded, because the control set that follows is different.

PART III OF VI

III – The Customer Lifecycle

When due diligence is triggered, what the measures actually are, how identity is verified for people and for businesses, what remote onboarding permits today, and how risk, screening and monitoring run for the life of the relationship.

§ 08 When is customer due diligence required?

§ 09 What does AMLR customer due diligence include?

§ 10 What are the KYC requirements for individuals?

§ 11 What are the KYB requirements for businesses?

§ 12 Can customers be onboarded remotely?

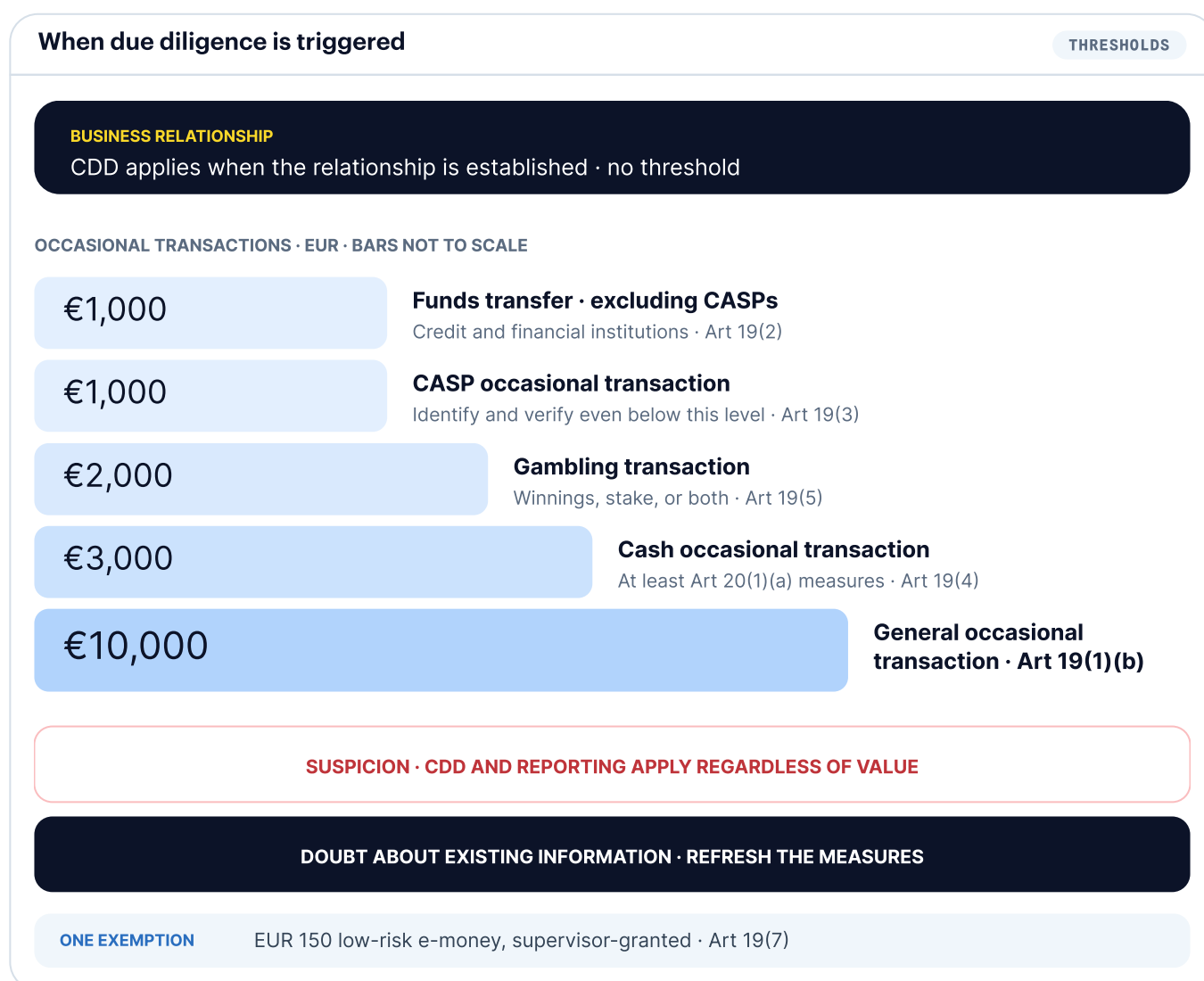
§ 13 How does risk affect due diligence?

§ 14 What screening does AMLR require?

§ 15 What does ongoing monitoring involve?

When is customer due diligence required?

CDD is required when a business relationship is established, when specified occasional transactions occur, when there is suspicion, and when an obliged entity doubts previously obtained identity information or doubts who it is dealing with.¹



LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 19(1)(a)-(f)

Same value, two separate provisions. The €1,000 funds-transfer trigger and the €1,000 CASP trigger are distinct — do not configure them as one rule. **Suspicion** makes CDD and reporting apply regardless of value, and **doubt** about existing information means refreshing the measures. One exemption: EUR 150 low-risk e-money, supervisor-granted [↓ Art 19\(7\)](#).

Transactions that appear separate must be treated together when they are linked. Controls should catch structuring across time, channels, accounts and related people.

For example, three cash payments of EUR 1,200 on consecutive days each sit below the EUR 3,000 cash trigger, but aggregate to EUR 3,600 above it. Whether your controls see one customer or three transactions is the whole question.¹

The cash trigger has a carve-out worth knowing: it does not apply where the Member State already operates a cash payment limit of EUR 3,000 or less under Article 80(2) and (3).²

The one exemption most summaries miss

Supervisors may exempt an obliged entity, fully or partly, from the Article 20(1)(a), (b) and (c) measures for electronic money on proven low risk. All four conditions must be met:³

Stored value	The instrument is not reloadable and stores no more than EUR 150 .
Closed use	It is used only for goods or services from the issuer, or within a defined network.
No cash out	It is not linked to a payment account and cannot be exchanged for cash or crypto-assets.
Monitoring	The issuer monitors transactions sufficiently to detect the unusual.

Note who grants it. This is a supervisor-granted exemption, not one you can assess for yourself.

KEY RULE

Different products and activities trigger different measures, and suspicion overrides every monetary threshold. There is no single "AMLR threshold" to configure.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 19(4) ² Art 19(4) ³ Art 19(7)(a)-(d)

What does AMLR customer due diligence include?

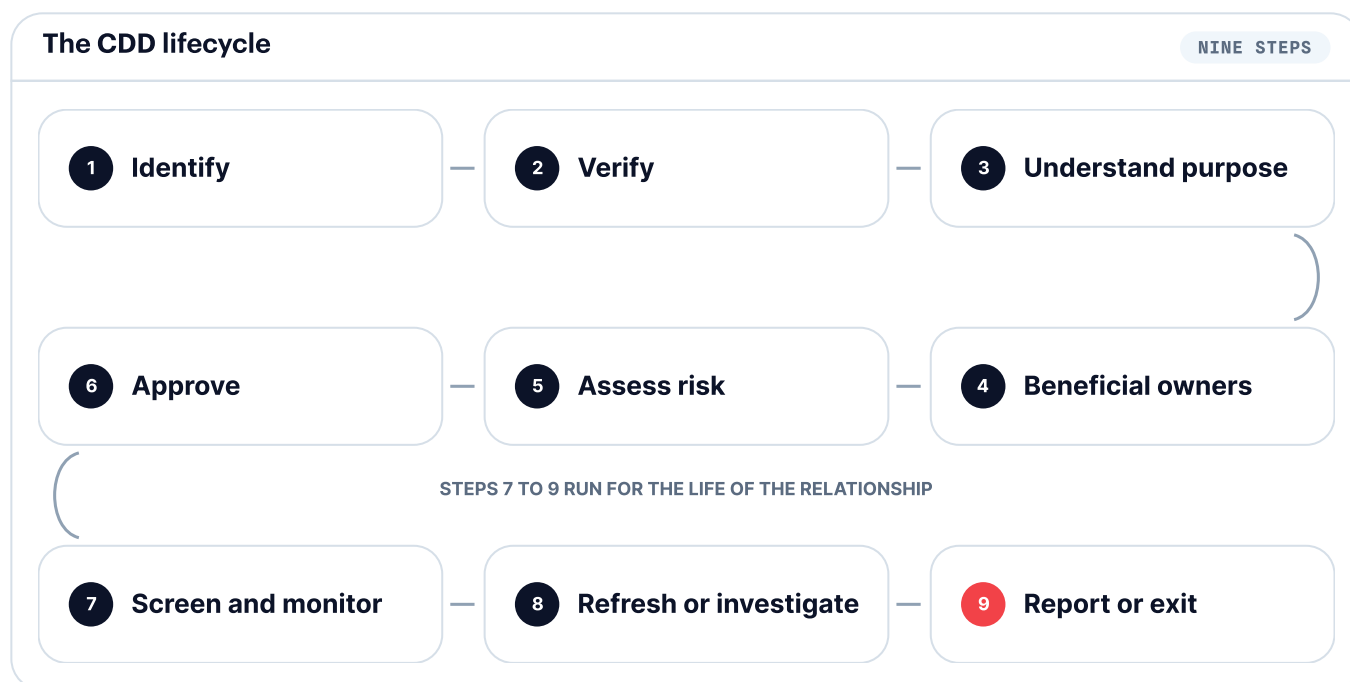
AMLR treats CDD as a continuing process, not a one-time document check. It is also worth keeping three articles distinct, because they are routinely collapsed into one.

Article 19 Says **when** CDD is required.

Article 20 Says **what** the measures are.

Article 22 Says **how** identity is identified and verified.

Calling Article 22 "the CDD article" is the most common citation error in AMLR commentary, and it will send you to the wrong provision when you need the right one.



The core measures are identifying and verifying the customer, identifying and verifying beneficial owners, assessing the purpose and intended nature of the relationship, and conducting ongoing monitoring.¹

KEY RULE

If CDD cannot be completed, do not establish or execute the relationship or transaction, and an existing relationship may need to end. Document the outcome, and consider whether the circumstances should be reported to the FIU.

Draft Level 2

The final Article 28 CDD RTS will add detail on required information and evidence. Its consultation is closed but the standard remains draft, so proposed document lists should not yet be presented as the final universal AMLR checklist.

What are the KYC requirements for individuals?

"Know your customer" is the operational process for performing CDD on a natural person. It is not a separate AMLR legal regime.

The KYC record, Article 22(1)(a)		LEGAL MINIMUM
 VERIFIED All names and surnames	 VERIFIED Place and full date of birth	
 VERIFIED Nationalities, or statelessness and refugee or subsidiary protection status where applicable Plus national identification number where applicable	 COLLECTED Usual place of residence, or postal address where there is no fixed residential address with legitimate residence in the Union Plus tax identification number where available	

Verification must use reliable and independent documents, data or information. A successful document check establishes identity attributes. Purpose, occupation, source of funds, PEP exposure and overall risk still need their own evidence.¹

Where a person acts for the customer, the firm must identify and verify the representative, identify the customer behind them, and confirm the authority to act. A mandate on file is not the same as evidence that the mandate is current.

KEY RULE

A passing document and biometric check answers *who* this person is. It does not answer why the relationship exists, where the money comes from, or how risky it is.

What are the KYB requirements for businesses?

"Know your business" applies CDD to legal entities and arrangements: legal existence, authority, ownership, beneficial owners, purpose and risk in one assessment.

The structural change under AMLR is that the duty is no longer one-sided. Previously the obliged entity investigated and the customer cooperated or did not. AMLR places statutory obligations on the customer entity, its beneficial owners, the entities in its ownership chain, its trustees and its nominees. KYB becomes a two-sided information exchange with deadlines on both sides.

TWO SIDES

OBLIGED ENTITY

Identify and verify the entity ↪ Art 22(1)(b)

Identify and verify beneficial owners
↪ Art 20

Report register discrepancies within 14 calendar days of detection ↪ Art 24(1)

Refresh customer information within 1 or 5 years ↪ Art 26(2)

CUSTOMER SIDE

Entity obtains BO information within 28 days of creation, updates promptly and within 28 days of change, and annually ↪ Art 62(2)

Entity reports to the central register without undue delay, changes within 28 days, verifies at minimum annually ↪ Art 63(2)

Beneficial owners and chain entities must supply what the entity needs ↪ Art 63(2)

Nominees must disclose nominator, the nominator's BOs and their own nominee status ↪ Art 66

Trustees report within 28 days and verify at least annually ↪ Art 64(2)

The six KYB questions

Question	What it establishes
Does the entity legally exist?	Official name, legal form, registration and governing law
Where does it operate?	Registered or official office and, if different, principal place of business and country of creation
Who can act for it?	Directors, representatives, mandates and authority
Who owns it?	Direct and indirect ownership through every material layer
Who controls it?	Voting, appointment, contractual or other control
Why does the relationship exist?	Business activity, purpose and expected transactions

Three data points older KYB models tend to miss

Article 22(1)(b) sets the legal-entity identification minimum, and three items in it are commonly absent from data models built for 4AMLD:

LEI	Legal Entity Identifier, where available.
Real operating base	Principal place of business where different from the registered or official office, plus country of creation.
Nominee status	Names of persons holding shares or a directorship in nominee form, including reference to their status as nominee shareholders or directors. ↪ Art 22(1)(b)(iv)

Companies, trusts, foundations, partnerships and collective-investment structures need different data models. A standard company checklist will not reliably identify all parties to a trust or similar arrangement. Central-register information supports CDD but does not ordinarily replace independent identification and verification.

When no beneficial owner can be identified

AMLR is stricter than the old senior-managing-official shortcut. Where all means under Articles 51 to 57 are exhausted, or there is "substantial and justified uncertainty", the entity keeps records of the actions taken **and** must supply:¹

A statement	That there is no beneficial owner, or that they could not be determined.
A justification	Of why, and of what the uncertainty consists of.
Full details	Of all senior managing officials.

AMLR also defines senior managing officials, which the previous directive did not. On the obliged-entity side, where verifying senior managing officials would signal that the firm doubts the ownership picture, it must abstain from that verification and instead record the steps taken and the difficulties encountered.²

KEY RULE

Where CDD information conflicts with beneficial-ownership register data, report to the *central registers* without undue delay and in any case within 14 calendar days of detection. Defined minor cases let you ask the customer first instead, but not in higher-risk cases.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 63(3)-(4) ² Art 22(2)

Is "perpetual KYB" required?

No. "Perpetual KYB" and "perpetual KYC" are industry terms. Neither appears in AMLR, and neither removes the periodic duty.

The practical position is more demanding than the label suggests. AMLR stacks five clocks:

01 • Entity	Updates its own BO information within 28 days of change, and annually. ↪ Art 62(2)
02 • Register	The entity reports register changes within 28 days and verifies at minimum annually. ↪ Art 63(2)
03 • Refresh	You refresh customer information within 5 years, or 1 year where enhanced measures apply. ↪ Art 26(2)
04 • Events	You review and update on three specific events, not on a schedule. ↪ Art 26(3)
05 • Discrepancy	You report register discrepancies within 14 days of detection . ↪ Art 24(1)

A five-year refresh cycle cannot detect a change the customer was obliged to register within 28 days, and the discrepancy clock only starts once you have looked. Event-driven KYB is not a legal requirement. It is the practical way to meet the requirements AMLR does impose.

For example, a customer entity whose beneficial owner changes in September must update its own record within 28 days and report the change to the register within 28 days. An obliged entity that last refreshed that customer in 2028 is not due to look again until 2033, and the 14-day discrepancy clock does not start until it does.¹

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 62(2) • Art 63(2) • Art 24(1)

Can customers be onboarded remotely?

Yes. Article 22(6) gives two routes and does not rank them. A proposed ranking exists, but only in draft Level 2, and the final text and the draft must be kept apart.

FINAL LAW

Art 22(6)

- (a) **Identity document route.** Identity document, passport or equivalent and, where relevant, information from reliable and independent sources.

EITHER / OR

- (b) **Electronic route.** Electronic identification means meeting Reg (EU) No 910/2014 at assurance level substantial or high, and relevant qualified trust services.

Article 22 itself does not rank the two routes.

DRAFT

Draft CDD RTS Art 7

- 1st Primary route.** Qualifying eID or qualified trust service, used first for non-face-to-face verification.
- 2nd Conditional fallback** where the primary route is unavailable or cannot reasonably be expected: remote document capture with safeguards covering quality, presenter match, integrity, interruptions, validity and retained evidence, and a justification to your supervisor.

KEY RULE

The priority-and-justification requirement sits in the *draft* Article 28 CDD RTS. Its consultation has closed, but it is not yet final adopted Level 2 law. Build for it, do not cite it as binding.

For example, an applicant onboarding at 22:00 during an outage of their national eID scheme can be verified under Article 22(6)(a) today, with no justification owed to anyone. Under the draft RTS the same journey would require a recorded reason why the primary route was unavailable. Building that field now costs little, and retrofitting it into a live journey later costs a great deal.

How eIDAS 2.0 and the EUDI Wallet connect to AMLR

AMLR never mentions the European Digital Identity Wallet. The connection runs through three instruments, and stating the chain explicitly is the difference between a claim you can defend and one you cannot.

FOUR LINKS

1

AMLR Art 22(6)(b)

Accepts electronic identification means meeting Reg (EU) No 910/2014 at assurance level substantial or high.

2

Regulation (EU) No 910/2014

This is eIDAS. AMLR points at it by number.

3

Regulation (EU) 2024/1183

Informally eIDAS 2.0. Amends 910/2014 and creates the European Digital Identity Wallet.

4

Wallets qualify under Art 22(6)(b) by reference

Wallets must meet Article 8 requirements at assurance level **high**  Reg 2024/1183 Art 5a(4)(d).
High satisfies the AMLR condition.

Each Member State must provide at least one Wallet within 24 months of the relevant implementing acts entering into force. The Regulation sets no calendar date, so treat any specific month you see quoted as derived from implementing-act timing rather than from the Regulation itself.¹

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Reg 2024/1183 Art 5a(1)

Three things the Wallet does not do. It does not create a hierarchy in Article 22(6), which remains route-neutral in final law. It does not remove the obliged entity's decision on whether the supplied attributes and assurance level meet the CDD requirement. And it answers who, not why: purpose, beneficial ownership and source of funds still need their own evidence.¹

If Wallets must be "high", what sits at "substantial"?

A fair question, and the answer matters more than it first appears. AMLR accepts electronic identification means at **substantial or high**. Wallets must be **high**. So what populates the substantial tier?

Notified national eID schemes. eIDAS 2.0 adds the Wallet; it does not abolish notification. Article 8(3) of Regulation (EU) No 910/2014, as amended, still sets minimum technical specifications for assurance levels low, substantial and high, and Article 9 still requires the Commission to publish the list of notified electronic identification schemes in the Official Journal and to publish amendments within one month.²

The substantial tier is therefore the existing installed base: national identity schemes, bank-identity schemes and equivalent means already notified by Member States and already listed.

KEY RULE

Article 22(6)(b) does not wait for Wallet rollout. A notified scheme already on the Official Journal list, assessed at substantial or high, satisfies the electronic route today.

There is a filter here that is easy to miss. Notified schemes span three assurance levels. AMLR accepts only two of them.

The assurance-level filter

THREE TIERS

LOW	Notified schemes exist at this level	NOT ACCEPTED
SUBSTANTIAL	Notified national eID schemes	ACCEPTED
HIGH	Notified schemes at high, and all EUDI Wallets - Reg 2024/1183 Art 5a(4)(d)	ACCEPTED

OPERATIONAL Check the Official Journal list of notified schemes and exclude anything notified at low before accepting it as an Art 22(6)(b) route.

Does a substantial-level eID need supplementing?

Not as a matter of Article 22(6)(b). Substantial is accepted on its own terms, and there is no obligation to top it up. Whether you *choose* to add measures is a risk question, governed by the ordinary rule that the extent and intensity of due diligence must reflect the customer, geography, product, transaction and delivery channel. A firm may reasonably decide that for a higher-risk customer a substantial-level eID alone is not enough, and layer additional verification on top. That decision is made under Articles 20 and 34, and it is documented and justified the same way any other risk-based calibration is.¹

Qualified trust services

Qualified trust services are the second limb of Article 22(6)(b) and are not interchangeable with electronic identification means.

Qualified signature	Links a person to signed data.
Qualified seal	Supports the origin and integrity of legal-person data.
Qualified timestamp	Establishes that data existed at a particular time.

None of them replaces purpose, beneficial-ownership or source-of-funds checks. Check qualified status against the national trusted list or the EU Trusted List Browser rather than a supplier's own description.

Where video identification sits

AMLR does not name video identification as a distinct route. It falls under Article 22(6)(a) as a means of obtaining information from reliable and independent sources, which means it is governed by the general verification standard rather than by a bespoke rule. Several Member States operate detailed national video-identification requirements today, and the EBA Remote Customer Onboarding Guidelines remain relevant transitional guidance until AMLA's replacement measures take effect. Under the draft CDD RTS, remote capture routes of any kind would become a conditional fallback requiring justification. That status is draft.

What to keep configurable

If you are building a remote onboarding flow now, keep these adjustable so the final RTS text can be applied without re-architecting the journey: which route is attempted first, and why; the recorded justification when a fallback is used; accepted assurance levels per product and risk tier; capture-quality and presenter-match thresholds; interruption and retry handling; and the evidence retained for supervisory review.

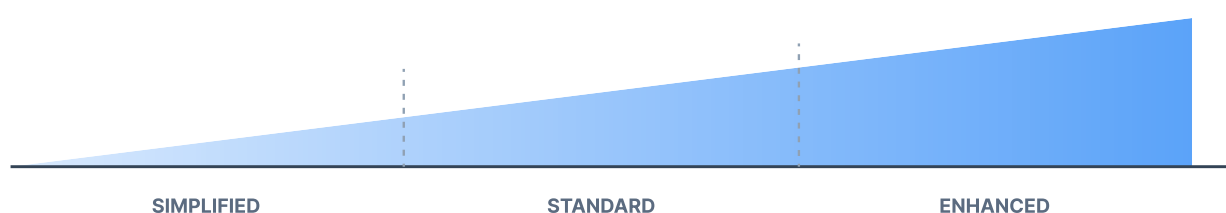
How does risk affect due diligence?

The extent and intensity of CDD must reflect risk, considering the customer, geography, product, transaction and delivery channel together.

FIG • 10 Three depths of due diligence

RISK-BASED

EXTENT AND INTENSITY OF MEASURES



Simplified

DEMONSTRABLY LOWER RISK

Adjust timing, extent or intensity; never skip CDD. Where verification is deferred for a qualifying low-risk relationship, completion cannot exceed **60 days**.

Standard

NORMAL RISK

Complete the core measures at risk-sensitive depth, with evidence for each.

Enhanced

HIGHER RISK OR PRESCRIBED

Additional evidence, senior approval, source-of-funds or wealth checks, transaction limits, closer monitoring.

Where verification is deferred for a qualifying low-risk relationship, it must be completed no later than 60 days after the relationship is established, and only where the specific lower risk identified justifies the postponement. Interim risk-management procedures are required in the meantime, such as limiting the amount, number or type of transactions.

For example, a qualifying low-risk relationship opened on 1 March with verification deferred and transaction limits applied must be fully verified by 30 April. On day 61 that file is not a backlog item, it is a breach.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

1 Art 20 • Annexes II-III 2 Art 33(1)(a) • Art 33(3)

Simplified due diligence must not be applied at all where there are doubts about veracity, where the lower-risk factors are no longer present, where monitoring excludes a lower-risk scenario, or where there is suspicion of money laundering, terrorist financing or sanctions evasion.¹

Source of funds	Where the money used in this relationship or transaction came from.
Source of wealth	How the customer's or beneficial owner's overall wealth was accumulated.

A numerical risk score can support consistency, but you have to be able to explain the rating, any material override, and the controls that follow from it.

Why the two definitions are kept apart

Enhanced measures can require either, and they are not answered by the same evidence. A payslip and a bank statement can establish the source of funds for one transaction while telling you nothing about how a fortune was built. Where Article 34 calls for source of wealth, a funds answer does not discharge it.

What screening does AMLR require?

"Screening" is several controls with different legal purposes and different consequences.

FOUR SCREENING CONTROLS

Control	Who or what is screened	What follows a match
Targeted financial sanctions ↳ Art 20(1)(d) ↳ Art 26(4)	Customers, beneficial owners and relevant controllers	Validate matches, then hand confirmed exposure to the sanctions process
Politically exposed persons ↳ Arts 42-46	PEPs, family members and known close associates	Senior approval, source-of-funds and wealth measures, enhanced monitoring
High-risk countries ↳ Arts 29-31 ↳ Art 35	Customer, ownership, operations and fund flows	Apply the prescribed enhanced measures or countermeasures
Adverse information	Reliable reputation information	Reassess risk, investigate the facts, consider whether suspicion exists

AMLR's sanctions-risk controls do not replace the separate legal duty to freeze assets and avoid making funds available under applicable restrictive measures. PEP status indicates higher risk. It is not evidence of wrongdoing.¹

Adverse media

"Adverse media screening" is not a standalone statutory duty under that name. Reliable public-source information can still affect customer risk, enhanced due diligence, ongoing review and suspicion assessment. Automated matches are not facts: identity resolution and human evaluation of source quality, recency and relevance come first.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 20(1)(d) · Art 26(4) · Arts 42-46

What does ongoing monitoring involve?

Article 26 requires firms to scrutinise transactions and activity, keep customer information current, and check that behaviour stays consistent with the customer's purpose and risk profile. It contains four distinct duties, and they run on different clocks.¹

FOUR DUTIES

Band 1 • Update

Max 1 year

Art 26(2)(a)

Customers to which **Section 4 enhanced due diligence measures apply**. This is narrower than "higher-risk customers" generally.

Band 2 • Update

Max 5 years

Art 26(2)(b)

All other customers.

Band 3 • Review

3 events

Art 26(3)

(a) A change in the relevant circumstances of a customer. (b) A legal obligation during the relevant calendar year to contact the customer to review beneficial-ownership information or to comply with Directive 2011/16/EU. (c) Becoming aware of a relevant fact pertaining to the customer.

Band 4 • Sanctions

Own clock

Art 26(4)

Regularly verify that the Art 20(1)(d) conditions are met, at a frequency commensurate with risk. For credit and financial institutions, **also upon any new designation**. This does not replace the obligation to apply targeted financial sanctions.

*The one-year and five-year figures are maximum intervals for **updating customer information**, not review targets. Three named events override the calendar, and sanctions verification runs regardless of either.*

Two precision points that matter when you build the schedule. First, Article 26(2) governs **updates of customer information**; the word "review" belongs to Article 26(3), which is a different duty with a different trigger.¹

Second, the one-year band is scoped to customers under Section 4 enhanced measures, not to every customer your internal model rates as higher risk. A customer can carry a high internal score without Section 4 applying, and that customer sits on the five-year clock.²

Two duties that run in parallel

DUTY 1 · CUSTOMER INFORMATION

- Keep identity, ownership and purpose current
- Respond to changes and risk events
- Update within 1 year under Section 4 measures
- Update within 5 years otherwise

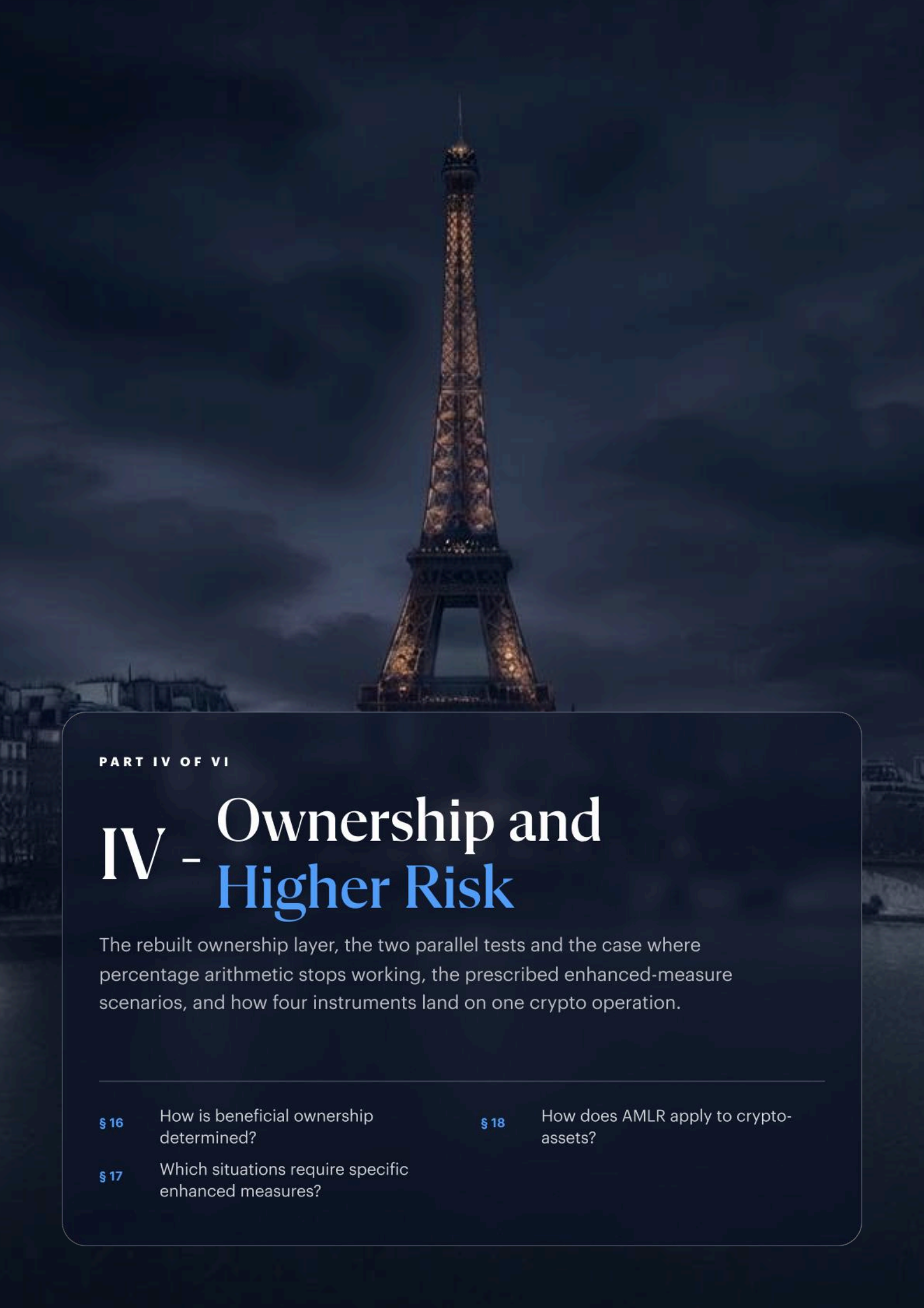
DUTY 2 · TRANSACTIONS AND ACTIVITY

- Detect unusual patterns and behaviour
- Investigate alerts in context
- Examine source of funds where necessary
- Decide whether activity should be reported

Automated monitoring needs scenario ownership, reliable data, calibration, validation and controlled case closure. Manual monitoring needs defined populations, frequency, trained reviewers and evidence. Neither model should rest on unexplained backlogs or blanket alert closure.

KEY RULE

Alerts closed in volume, with no recorded reasoning, are read as a control that is not working, whatever the closure rate says.

A full-page background image of the Eiffel Tower in Paris, France, illuminated at night against a dark, cloudy sky. The tower's golden lights contrast with the dark environment.

PART IV OF VI

IV – Ownership and Higher Risk

The rebuilt ownership layer, the two parallel tests and the case where percentage arithmetic stops working, the prescribed enhanced-measure scenarios, and how four instruments land on one crypto operation.

§ 16

How is beneficial ownership determined?

§ 18

How does AMLR apply to crypto-assets?

§ 17

Which situations require specific enhanced measures?

How is beneficial ownership determined?

A beneficial owner is the natural person who ultimately owns or controls a legal entity or arrangement. AMLR runs two tests, and they are parallel rather than sequential.

The general corporate indicator is **25% or more** of the shares, voting rights or other ownership interest, including rights to a share of profits, other internal resources or liquidation balance, held directly or indirectly.¹

Control is assessed "independently of and in parallel to" the existence of an ownership interest. Control through ownership interest means 50% plus one. Control via other means carries **no percentage floor at all**: a majority of voting rights whether or not shared by persons acting in concert, the right to appoint or remove a majority of the board, relevant veto or decision rights attached to shares, decisions on profit distribution or asset shifts, and formal or informal agreements including relationships between family members and nominee arrangements.²

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 52(1) ² Art 51 · Art 53(2)(c) · Art 53(3)-(4)

Resolving the beneficial owner

THREE TESTS

MAP DIRECT AND INDIRECT OWNERSHIP THROUGH EVERY LAYER

TEST 1 · OWNERSHIP

Natural person holds 25% or more, directly or indirectly?

YES

Identify and verify that person

Independent evidence, not registry data alone

NO

TEST 2 · CONTROL

Control through voting, board, contract or dominant influence?

YES

NO

TEST 3 · EXHAUSTION

Every identification means exhausted and documented?

YES

Record senior managing officials

STATUTORY FALLBACK · LAST RESORT

NO AT TEST 3 · CONTINUE MAPPING, DO NOT DEFAULT TO A DIRECTOR

The senior-managing-official fallback is not permission to call a director the UBO because a database found nothing. It requires exhausted investigation and documented uncertainty.

Indirect ownership, and the case where arithmetic does not work

Indirect ownership is calculated by multiplying holdings through each chain and adding the chains together. All shareholdings at every level count.¹

But that arithmetic is expressly disappplied where Article 54 applies. Where a multi-layered structure has ownership interest and control **coexisting at different layers of a chain**, the beneficial owners become the natural persons controlling the entities that hold a direct ownership interest, and the natural persons with an ownership interest in the entity that controls the corporate entity.²

PURE OWNERSHIP CHAIN	OWNERSHIP AND CONTROL COEXIST · ART 54
40% Natural person	40% Natural person
40% Holding company	60% Holding company, control through ownership interest
• Customer	• Customer
Multiply and add: $40\% \times 40\% = 16\%$. Below the threshold, so no beneficial owner on the ownership limb.	Arithmetic gives 24% and reports nothing. But 60% is control, so Art 54 displaces the calculation: the 40% holder is a beneficial owner.

One method does not cover both. A rule engine that only multiplies and adds will miss every Article 54 structure it meets.

Where a legal arrangement or an Article 57 entity sits in the chain, the beneficial owners are the beneficial owners of that arrangement or entity.³

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 52(1) ² Art 54 ³ Art 55

Trusts and complex structures

Trusts and similar arrangements need function-based identification. Relevant persons can include settlors, trustees, protectors, beneficiaries or classes of beneficiaries, and any person exercising ultimate control. A company-shaped checklist will miss several of these roles entirely.¹

For a complex structure, map each ownership layer, calculate indirect interests, identify the natural persons behind intermediate entities, examine nominee arrangements, and understand the commercial rationale. A structure whose only apparent purpose is to obscure ownership is itself a risk indicator.

Ownership deadlines to build into the operating model

Deadline	Duty	Article
28 calendar days	Entity obtains BO information after creation	↳ Art 62(2)
Promptly, in any case 28 days	Entity updates its own BO information after any change	↳ Art 62(2)
Without undue delay, in any case 28 days	Report a change to the central register	↳ Art 63(2) ↳ Art 64(2) ↳ Art 67(5)
At minimum annually	Entity verifies it holds up-to-date BO information	↳ Art 63(2)
At least annually	Trustee verifies the wider information set held	↳ Art 64(2)
Without undue delay, in any case 14 days	Obligated entity reports a register discrepancy after detection	↳ Art 24(1)
5 years	Retention of specified ownership records after cessation	↳ Art 63(6) ↳ Art 64(1)

Note that the initial register report differs by entity type. A legal entity reports "without undue delay after its creation" with no 28-day cap. A trustee reports without undue delay **and in any case within 28 calendar days**.²

KEY RULE

A register entry supports the assessment. It is not, on its own, independent verification of who ultimately owns or controls the customer.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Arts 58-60 ² Art 63(2) · Art 64(2)

Which situations require specific enhanced measures (EDD) ?

Some relationships require prescribed enhanced due diligence in addition to the general customer-risk assessment.¹

Situation	What is required	Article
High-risk third country	Additional customer, ownership, purpose, funds, wealth, approval and monitoring measures	↳ Arts 29-31
Correspondent banking	Respondent ownership, reputation, supervision, controls and responsibilities	↳ Art 36
Correspondent crypto relationships	Equivalent measures for CASP correspondent relationships	↳ Art 37
Shell institution	Prohibited relationship; guard against indirect access	↳ Art 39
Self-hosted crypto address	Ownership or control, transfer risk and proportionate mitigation	↳ Art 40
Residence-by-investment applicant	Funds, wealth, PEP exposure, intermediaries and structure	↳ Art 41
PEP or former PEP	Senior approval, source-of-wealth and funds evidence, enhanced monitoring	↳ Arts 42-46
Life or investment insurance	Beneficiary identity, ownership and PEP exposure	↳ Art 44 ↳ Art 47
Higher-risk high-net-worth service	Prescribed gate, see overleaf	↳ Art 34(5)

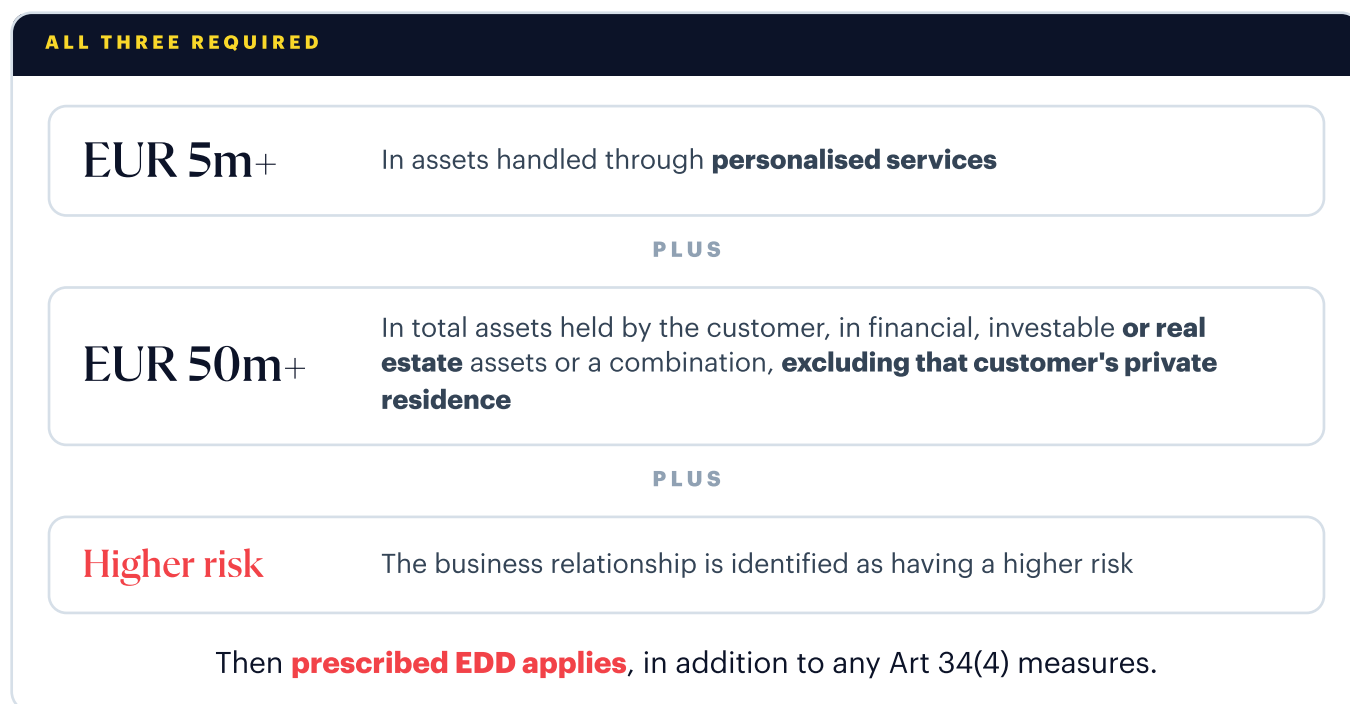
Former PEPs

Mitigating measures continue until the risk no longer exists, and "in any case for **not less than 12 months** following the time when the individual ceased to be entrusted with a prominent public function". The clock runs from the person leaving the function, not from your last review. The duty is to apply one or more of the Article 34(4) measures, not the full PEP regime. It applies equally to a new customer who formerly held such a function.²

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 34 ² Art 45(1)-(3)

The prescribed high-net-worth gate



Three corrections matter here. The Regulation contains **no annual qualifier**: the trigger is the value of assets handled through personalised services, not an annual flow. The exclusion is the customer's **private residence**. And the duty binds only **credit institutions, financial institutions and trust or company service providers**, not obliged entities generally.¹

Below any one of the three elements, the prescribed rule does not bite and the general risk-based approach applies. For example, a customer holding EUR 60,000,000 in total assets but running only EUR 2,000,000 through personalised services fails the first limb. The prescribed gate does not apply, and the relationship is assessed under the general risk-based approach like any other.²

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 34(5) ² Art 34(5)

How does AMLR apply to crypto-assets?

Crypto-asset service providers operate AMLR and the Transfer of Funds Regulation together. One customer, one transfer, two rulebooks. A third and a fourth instrument sit alongside them, and keeping the four apart is the single most useful thing a crypto compliance team can do with AMLR.

ATTRIBUTION

AMLR

Reg 2024/1624

LIFECYCLE DUTIES

CDD at EUR 1,000 occasional ↪ [Art 19\(3\)](#), self-hosted address risk mitigation ↪ [Art 40](#), anonymity prohibitions ↪ [Art 79](#), correspondent CASP relationships ↪ [Art 37](#)

TFR

Reg 2023/1113

TRANSFER DUTIES · APPLIES SINCE 30 DECEMBER 2024

Originator and beneficiary information, transfer-message completeness, missing-information handling, travel-rule records

MiCA

Reg 2023/1114

AUTHORISATION AND DEFINITIONS

What a CASP is, and who may operate as one

AMLD6

Dir 2024/1640

NATIONAL MACHINERY

Registers, FIU, supervision

Attributing a rule to the wrong instrument is the most common error in crypto AML commentary.

What AMLR does and does not prohibit

Self-hosted addresses are **not banned**. CASPs must identify and assess the money laundering and terrorist financing risk of transfers to or from a self-hosted address, then apply mitigating measures commensurate with that risk. One or more of:¹

Identify	Risk-based identification and verification of the originator or beneficiary, or their beneficial owner.
Trace	Additional information on the origin and destination of the crypto-assets.
Monitor	Enhanced ongoing monitoring of transactions with a self-hosted address.
Or other	Any other measure that mitigates the risk.

There is no fixed threshold in this article. The "verify who controls the wallet above EUR 1,000" rule that circulates in summaries is the **Transfer of Funds Regulation**, not AMLR.

Anonymity is where AMLR does prohibit. Credit institutions, financial institutions **and CASPs** are prohibited from keeping anonymous bank and payment accounts, anonymous passbooks, anonymous safe-deposit boxes or **anonymous crypto-asset accounts**, as well as any account otherwise allowing the anonymisation of the account holder or "the anonymisation or increased obfuscation of transactions, including through **anonymity-enhancing coins**".²

KEY RULE

Article 79(1) prohibits obliged entities from *keeping accounts* that enable anonymisation, including through anonymity-enhancing coins. It does not criminalise privacy coins, ban self-custody, or outlaw non-custodial software.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 40(1) ² Art 79(1)

"AMLR bans privacy coins" is a misreading of an account-level prohibition. Existing anonymous accounts, passbooks, safe-deposit boxes and crypto-asset accounts must be subject to CDD before they are used in any way.¹

Analytics is not identity

Blockchain analytics supports risk assessment but is not an infallible identity source. Attribution confidence, chain coverage, clustering assumptions, privacy features and false positives all need governance.



PART V OF VI

V - Reporting, Data and Limits

Suspicion reporting, the threshold reports that have nothing to do with suspicion, what may be shared, how AMLR meets GDPR, and the anonymity and cash restrictions.

§ 19 When must suspicious activity be reported?

§ 20 What must be reported on high-value goods?

§ 21 When can AML information be shared?

§ 22 How does AMLR interact with GDPR, AI and recordkeeping?

§ 23 What anonymity and cash restrictions does AMLR introduce?

When must suspicious activity be reported?

An obliged entity must report without delay to its national FIU when it knows, suspects or has reasonable grounds to suspect that funds or activity are connected to criminal conduct or terrorist financing. The duty applies irrespective of amount and can cover attempted transactions.¹

From anomaly to report

Unusual fact or activity

Internal assessment

Preserve facts, transactions, ownership context and reasons

Suspicion threshold met?

NO

Document and keep monitoring

Escalate if the picture changes



NO TIPPING OFF · ART 73

Never reveal that a report has been or will be made, or that FIU analysis is under way.

YES

Report promptly to the FIU

WITHOUT DELAY · ANY AMOUNT · ART 69

Refrain where required · Art 71

Three-working-day rule if no FIU instruction, subject to statute and national procedure

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 69

Your internal assessment should preserve the relevant facts, transactions, ownership context, explanations, and the reason for the conclusion. Staff do not need to prove the underlying crime before escalating a concern, and a policy that implies otherwise suppresses reporting.

The tipping-off constraint has to be designed into customer-facing scripts, complaint handling, account-closure messaging and automated notifications, not bolted on afterwards.¹

National filing portals and procedures remain important even as AMLA develops a common reporting-format standard. Firms operating in several Member States should treat filing mechanics as a per-country workstream.

KEY RULE

A transaction that never completed can still require a report. The duty attaches to suspicion, not to settlement.

What must be reported on high-value goods?

Alongside suspicion-based reporting, AMLR introduces a threshold-based reporting duty that has nothing to do with suspicion. It is easy to miss because it sits at the end of the reporting chapter.

Persons trading in high-value goods must report to the FIU all transactions involving the sale of the following goods **when those goods are acquired for non-commercial purposes**.¹

THREE TIERS

EUR 250,000 MOTOR VEHICLES	EUR 7,500,000 WATERCRAFT	EUR 7,500,000 AIRCRAFT
--	--	--

● **Condition: acquired for non-commercial purposes**

Two points that summaries routinely drop. The duty is not limited to the trader: **credit institutions and financial institutions** that provide services in relation to the purchase or transfer of ownership of these goods also report the transactions they carry out for their customers. And there is no fixed EU deadline: reporting is carried out "within the deadlines imposed by the FIU".²

The commercial-purpose condition does real work. A dealership buying stock is outside paragraph 1. A private buyer at or above the threshold is inside it. For example, a dealer acquiring three vehicles at EUR 300,000 each for resale reports nothing under this article. A private buyer acquiring one of those same vehicles at EUR 300,000 triggers the report.³

These same thresholds also appear in Article 67 as one of the triggers that pull a **foreign** legal entity or arrangement into an EU central register.⁴

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 74(1) ² Art 74(2) · Art 74(3) ³ Art 74(1) ⁴ Art 67(1)(c)

When can AML information be shared?

AMLR permits defined information sharing within groups and through qualifying information-sharing partnerships, with a clear AML/CFT purpose, restricted access, security, governance and data-protection safeguards.¹

Four decisions you must still make yourself

- ✗ A customer risk conclusion
- ✗ Refusing or terminating a relationship
- ✗ Suspending a transaction
- ✗ Your own FIU reporting decision

Each of those decisions has to rest on the obliged entity's own assessment. Shared intelligence can direct attention, prompt a review or corroborate a finding, but the accountable decision stays with the firm that makes it.

The tipping-off prohibition still applies. Information that would disclose that a suspicious-activity report exists, or that an FIU analysis is under way, can be shared only where a specific legal exception permits it.²

Governance to put in place first

- A defined AML/CFT purpose
- A lawful basis
- Role-restricted access
- Logging
- Retention limits
- Security controls
- An assessment of accuracy and provenance
- A documented escalation route for disputes

KEY RULE

Sharing improves what you can see. It transfers nothing: not the decision, not the accountability, not the reporting duty.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 75 · Art 16 ² Art 73

How does AMLR interact with GDPR, AI and recordkeeping?

AMLR provides a legal framework for necessary AML/CFT data processing. It does not remove GDPR principles.¹

Principle	What it means in practice
Purpose limitation	Do not repurpose AML data for unrelated commercial activity
Data minimisation	Collect the attributes needed for the legal and risk outcome
Accuracy	Separate official facts, credible reporting, allegations and automated inference
Sensitive-data protection	Restrict special-category and criminal-offence data
Human intervention	Give reviewers evidence and authority to change automated outcomes
Security	Limit access, log activity and protect reporting confidentiality

Automation can extract documents, triage alerts, score risk and identify patterns. It does not transfer accountability to the model or the provider. Where meaningful human intervention is required, the reviewer must understand the evidence and be able to alter the decision. An approval click alone is not enough.

Record keeping requirements

5 + UP TO 5

REQUIRED

5 years

Running from termination of the business relationship, the carrying out of the occasional transaction, **or refusal** to enter a relationship or carry out an occasional transaction.

↳ Art 77(3)

CONDITIONAL EXTENSION

Up to 5 more

Only where a **competent authority requires it on a case-by-case basis**, and only where necessary for the prevention, detection, investigation or prosecution of ML/TF.

↳ Art 77(3)

SEPARATELY A transitional Member State option exists for legal proceedings pending on 10 July 2027

↳ Art 77(4)

Personal data must be deleted on expiry of the five-year period, without prejudice to retention periods set by other Union or national law compliant with GDPR.¹

Your records should be able to reconstruct what was known, which sources were used, how ownership and risk were assessed, who approved the outcome, and what monitoring or reporting action followed.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 77(3)

What anonymity and cash restrictions does AMLR introduce?

AMLR prohibits anonymous instruments and puts an EU-wide ceiling on professional cash payments.

Prohibited or restricted instruments

Anonymous bank and payment accounts, anonymous passbooks, anonymous safe-deposit boxes and anonymous crypto-asset accounts, plus any account allowing anonymisation or increased obfuscation of transactions. Acquirers must not accept payments made with anonymous prepaid cards issued in third countries, subject to any RTS adopted under Article 28.¹

Bearer shares now carry dates

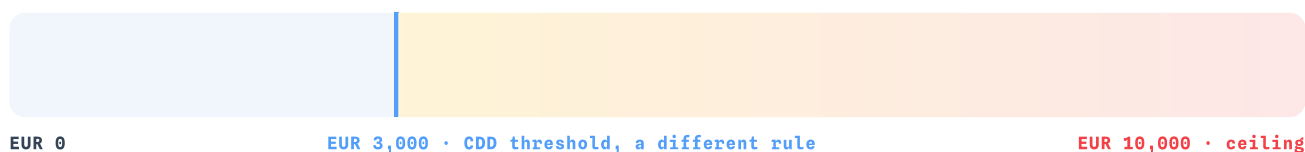
Companies are prohibited from issuing bearer shares. Existing bearer shares must be converted into registered shares, immobilised, or deposited with a financial institution **by 10 July 2029**. Where that does not happen, all voting rights and rights to distribution are automatically suspended until conversion, immobilisation or deposit. Shares still not dealt with **by 10 July 2030** are cancelled, reducing share capital accordingly. Listed companies and shares issued as intermediated securities are carved out. Bearer share warrants that are not in intermediated form are prohibited.²

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 79(1) · Art 79(2) ² Art 79(3)

The cash ceiling

The Article 80 cash ceiling



THE CEILING

EUR 10,000 on cash accepted or made by persons trading in goods or providing services, single operation or several which appear to be linked. - Art 80(1)

NATIONAL FLOORS

Member States may adopt lower limits after ECB consultation; pre-existing lower national limits continue to apply. - Art 80(2)-(3)

CARVE-OUT (A)

Payments between natural persons **not acting in a professional capacity**. - Art 80(4)

CARVE-OUT (B)

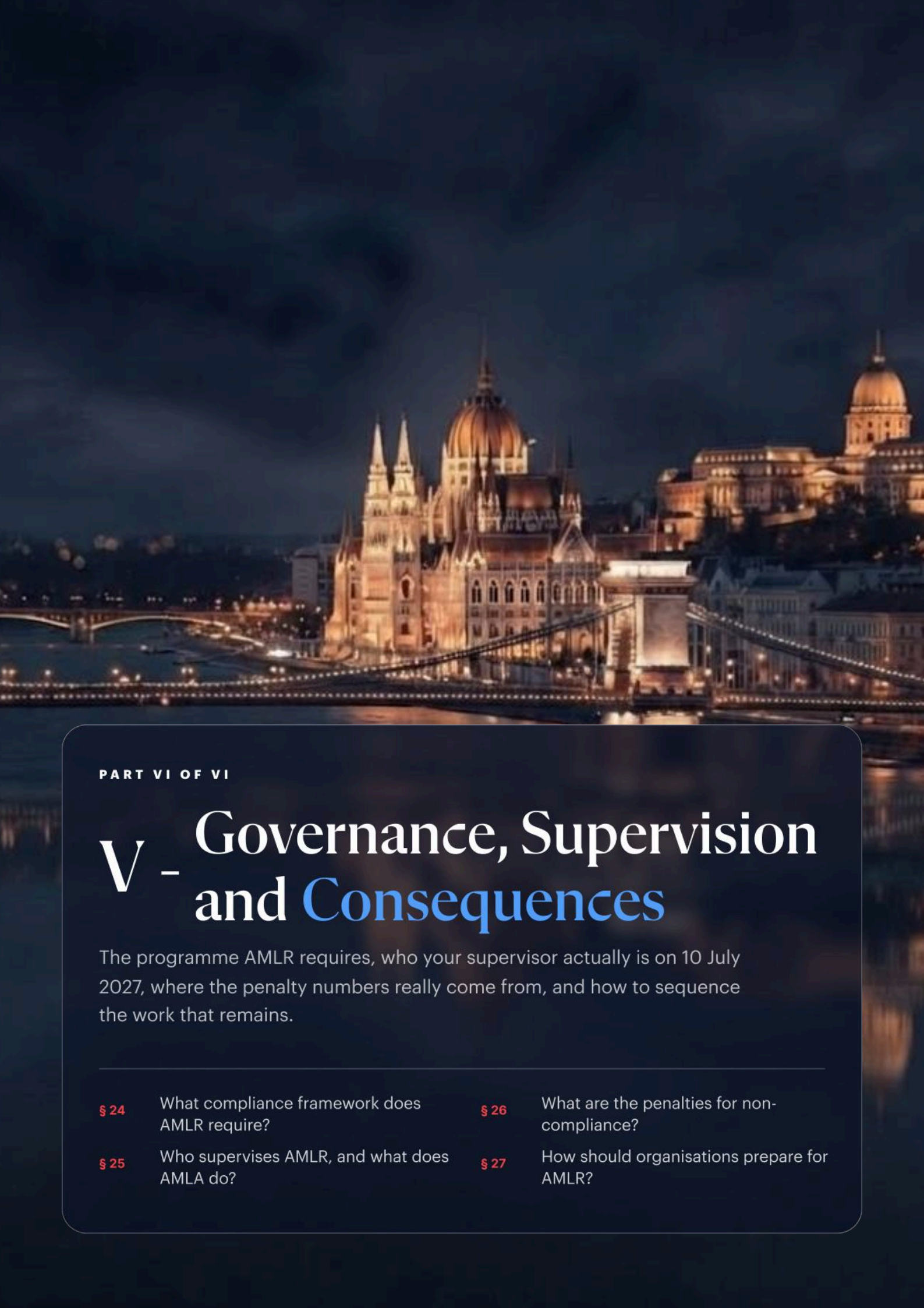
Payments or deposits at the premises of credit institutions, e-money issuers and payment service providers. **Above the limit these must be reported to the FIU** within the deadlines the FIU imposes. - Art 80(4)

OVERRIDE Suspicion triggers CDD and reporting at any value.

The cash ceiling is not the CDD threshold. A EUR 3,000 cash transaction can trigger identification and verification even though it sits below the payment ceiling, and suspicion triggers CDD and reporting at any value. If you operate across Member States you need a country matrix covering lower national limits, exclusions, linked payments, mixed payment methods and refund controls.¹

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 19(4) · Art 80(1)



PART VI OF VI

V - Governance, Supervision and Consequences

The programme AMLR requires, who your supervisor actually is on 10 July 2027, where the penalty numbers really come from, and how to sequence the work that remains.

§ 24 What compliance framework does AMLR require?

§ 25 Who supervises AMLR, and what does AMLA do?

§ 26 What are the penalties for non-compliance?

§ 27 How should organisations prepare for AMLR?

What compliance framework does AMLR require?

AMLR requires a risk-based and proportionate programme. A smaller obliged entity may use simpler controls than a cross-border bank, but it must still achieve the required outcomes and prove that the controls work.¹

Six elements of the framework

01 • Oversight	Management oversight of the programme.
02 • Risk	Business-wide risk assessment.
03 • Controls	Policies, procedures and controls.
04 • Lifecycle	The customer lifecycle, end to end.
05 • Detection	Monitoring and reporting.
06 • Assurance	Testing and assurance.

The business-wide risk assessment should reflect actual customers, geographies, products, services, transactions, delivery channels and technology, and connect identified risk to control design and investment rather than read as a generic description of the sector.²

The compliance officer and the management body

AMLR separates responsibility rather than leaving it to organisational preference. The management body carries overall accountability. A member of the management body is designated as the compliance manager responsible for implementation. A compliance officer runs day-to-day compliance, reports to the management body, and must have the standing, resources and access to discharge the role.³

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Arts 9-18 ² Art 10 ³ Art 11

Staff must be made aware of the requirements that apply to their role, with training proportionate to the risks and to what the person actually does. Employee integrity measures and protected internal reporting routes are part of the framework, not optional additions.¹

Groups apply group-wide policies, procedures and controls, including information sharing for AML/CFT purposes within the group. Where a third country's law prevents implementation, the conflict must be escalated and additional measures applied.²

Outsourcing and reliance are not the same thing

OUTSOURCING · ART 18

A provider may perform permitted tasks

The obliged entity remains accountable

Decisions reserved to the obliged entity stay with it

RELIANCE · ARTS 48-50

Under defined conditions, CDD performed by another obliged entity may be used

Responsibility remains with you

The information and evidence must be available

Neither route transfers accountability. In both cases the obliged entity has to produce the underlying information and evidence on request, and demonstrate that the arrangement was assessed, documented and monitored. Contractual language alone is not a control.

KEY RULE

Proportionality governs how a control is built, never whether the outcome is achieved. A small firm may run simpler processes, but it still has to evidence them.

Who supervises AMLR, and what does AMLA do?

AMLA is the most misunderstood part of the package. The short answer is that for most obliged entities, the supervisor on 10 July 2027 is the same national authority as today.

The Anti-Money Laundering Authority was created by Regulation (EU) 2024/1620, which applies from **1 July 2025**. The Commission was responsible for its establishment and initial operation until 31 December 2025.¹

TWO TIERS

AMLA DIRECT SUPERVISION

Up to 40

Credit and financial institutions and groups whose **residual** risk profile is classified high. Up to 40 in the first selection round; a greater number may be agreed subsequently.

AMLA Reg Art 13(1)–(2) · Art 106(2)

NATIONAL SUPERVISORS

Everyone else

Many thousands of obliged entities across all sectors. Powers, resources, risk-based supervision, colleges and cooperation sit in AMLD6.

AMLD6 Arts 37–52

TIMING First selection commences by 1 July 2027, concludes within six months, and direct supervision begins six months after the list is published ↪ **AMLA Reg Art 13(4)**

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ AMLA Reg Art 108 · AMLA Reg Art 107

For everyone outside the selected cohort, AMLA still matters, but indirectly. It writes regulatory and implementing technical standards, issues guidelines, oversees national supervisors and supports FIU cooperation. The Article 28 CDD RTS and the Article 26(5) monitoring guidelines are AMLA products, and they will shape day-to-day practice far more than direct supervision will.

KEY RULE

AMLA is not permanently capped at 40 entities. Article 13(2) allows a specific different number *greater than* 40 to be agreed with supervisors. The hard 40 applies only to the first selection process.

What this means for your 2027 planning

If you are not in the selected cohort, nothing about your supervisory relationship changes on 10 July 2027: the same national authority, the same reporting lines, the same inspection cycle. What changes is the rulebook it supervises you against, and the Level 2 measures AMLA writes underneath it. Track the standards, not the selection list.

What are the penalties for non-compliance?

Penalties sit in two instruments, and neither of them is AMLR.

KEY RULE

AMLR Article 68 is titled "Penalties" but covers *Chapter IV*, beneficial ownership transparency, only. It delegates to Member States and contains no monetary figure. Citing it for the EUR 10 million number is wrong.

AMLD6 requires Member States to make pecuniary sanctions available for serious, repeated or systematic breaches of AMLR Chapter II (internal policies), Chapter III (customer due diligence), Chapter V (reporting) and Article 77 (record retention), and for non-compliance with administrative measures.¹

Tier 1 Obligated entities generally

AMLD6 Art 55(2)

Maximum sanctions of **at least twice the benefit** derived from the breach where determinable, **or at least EUR 1,000,000**, whichever is higher.

Tier 2 Credit and financial institutions

AMLD6 Art 55(3)

Legal persons, **at least EUR 10,000,000 or 10% of total annual turnover, whichever is higher**.
Natural persons, **at least EUR 5,000,000**.

Tier 3 Entities under AMLA direct supervision

AMLA Reg Art 22

Basic amounts by breach category, then capped at **10% of total annual turnover** for CDD, group-policy and reporting breaches, and at **EUR 10,000,000** for all other breaches.

*These are **minimum maxima**. They are floors on the ceiling each Member State must provide, not the sanction a firm will face.*

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ AMLD6 Art 55(1)

Three qualifications travel with the headline number. AMLD6 says "maximum pecuniary sanctions of **at least**", which makes it a floor on the ceiling. The EUR 10 million and 10% tier applies **only to credit and financial institutions**; every other obliged entity sits on the EUR 1 million tier. And Member States may empower authorities to exceed these amounts, while ability to pay must be taken into account.¹

Tier 3 is structured differently, and the difference matters

For entities under AMLA direct supervision the structure is not "EUR 10 million or 10%, whichever is higher". AMLA sets a basic amount within ranges that vary by breach type and by whether the breach spans one Member State or several, adjusts it using aggravating and mitigating coefficients, and then applies one of two separate caps depending on the breach category.²

Writing the two regimes as though they share a formula is the most common error in AMLR penalty commentary.

Periodic penalty payments

Less discussed, and operationally sharper. Where an obliged entity fails to comply with certain administrative measures within the deadline, supervisors may impose periodic penalty payments until it does. They are capped at **3% of average daily turnover** for legal persons, or **2% of average daily income** for natural persons. They run for no more than six months, extendable once by a further six months.³

A sanction is an event, a periodic penalty is a meter

A sanction is a single event. A periodic penalty payment accrues daily until the control is fixed.

How should organisations prepare for AMLR?

National supervisors remain responsible for most obliged entities. AMLA will coordinate the EU system and directly supervise only a selected group of higher-risk cross-border financial entities, with preparations for the 2027 selection exercise under way and direct supervision expected from 2028.

Eight readiness workstreams

- | | |
|--|---|
| <p>01 Scope. Entity, branch, service and national-overlay register.</p> | <p>05 Onboarding. Future-state CDD, KYC/KYB and remote process.</p> |
| <p>02 Requirements. Article-to-control inventory with accountable owners.</p> | <p>06 Lifecycle controls. Validated screening, monitoring and reporting.</p> |
| <p>03 Risk. Updated business-wide risk assessment.</p> | <p>07 Governance. Updated roles, outsourcing, reliance, training, assurance.</p> |
| <p>04 Customer data. Remediated identity, ownership and stale records.</p> | <p>08 Regulatory change. Level 2 tracker and controlled implementation plan.</p> |

A gap analysis is the practical starting point, and it is more specific than a generic readiness assessment. Four questions produce most of the findings:

- | | |
|------------------------------------|---|
| <p>01 • The operator</p> | <p>Does any rule, form or engine still test beneficial ownership at > 25% rather than >= 25%? ↓ Art 52(1)</p> |
| <p>02 • The clock</p> | <p>Can you evidence the date on which each customer's information was last updated, and does any population exceed the one-year or five-year cap? ↓ Art 26(2)</p> |
| <p>03 • The data model</p> | <p>Do your KYB records capture LEI, principal place of business and nominee status? ↓ Art 22(1)(b)</p> |
| <p>04 • The audit trail</p> | <p>Can you produce, for any customer, the reasoning behind a closed alert and the person who closed it?</p> |

Where the work concentrates, by sector

Credit and financial institutions verify sanctions on any new designation, not only at review points, and sit on the penalty band of EUR 10,000,000 or 10% of total annual turnover. A few dozen of these institutions will also fall into AMLA's directly supervised cohort.¹

Crypto-asset service providers are the only sector running two rulebooks on different clocks. TFR travel-rule duties have applied since 30 December 2024. AMLR then adds the EUR 1,000 occasional-transaction trigger, self-hosted address risk mitigation, correspondent duties and the anonymity prohibitions from 10 July 2027. Keeping the attribution straight between the two instruments is most of the work.²

Trust and company service providers sit inside the Article 34(5) high-net-worth gate alongside credit and financial institutions, and they are the sector most exposed to the rebuilt ownership layer in Articles 51 to 55.³

Estate agents and real-estate professionals should note that both parties to the transaction count as customers. That doubles the due-diligence population on every deal.⁴

Traders in high-value goods acquire a reporting duty they have not had before: threshold reports to the FIU at EUR 250,000 for motor vehicles and EUR 7,500,000 for watercraft and aircraft, on non-commercial acquisitions only, plus the EUR 10,000 cash ceiling.⁵

Football agents and clubs have two extra years, to 10 July 2029. Clubs should establish whether a Member State exemption applies before building anything.⁶

KEY RULE

Scope analysis, governance, data remediation, ownership logic, architecture and testing can proceed now. Keep draft-dependent details configurable and give them a final-text review before closing implementation.

LEGAL BASIS (AMLR UNLESS ANOTHER INSTRUMENT IS NAMED)

¹ Art 26(4) · AMLD6 Art 55(3) · AMLA Reg Art 13 ² Art 19(3) · Art 40 · Art 37 · Art 79

³ Art 34(5) · Arts 51-55 ⁴ Art 19(6)(c) ⁵ Art 74(1) · Art 80(1) ⁶ Art 90 · Art 5

Where Shufti fits the AMLR lifecycle

AMLR does not split neatly into products. It runs as one lifecycle: identify, verify, establish ownership, assess risk, screen, monitor, refresh, report.

Shufti is a glocal platform that runs that full compliance lifecycle, from sign-up and onboarding through authentication and monitoring to remediation, across **240+ countries and territories** and **10,000+ document types actively verified each month**. For remote onboarding it supports both Article 22(6) routes, and it is prepared to accept European Digital Identity Wallet attributes as EUDI Wallets become available.

Capability	Where it lands in AMLR
Identity Verification	The Art 22(6)(a) route, and the compliant fallback where a primary electronic route is unavailable. Document and biometric checks against reliable, independent sources. Single-selfie passive liveness assessed at iBeta PAD Level 3 under ISO/IEC 30107-3 on both iOS and Android, returning 0% APCER and 0% BPCER. Shufti was the first European company to achieve that conformance. shuftipro.com/identity-verification/
KYC	Art 22(1)(a) attribute capture and verification. shuftipro.com/know-your-customer/
KYB	Art 22(1)(b) entity data, UBO mapping across Arts 51 to 55, and the register-discrepancy duty in Art 24. shuftipro.com/know-your-business/
AML Screening	Sanctions, PEP and adverse-information screening with human-review workflows for identity resolution and escalation. shuftipro.com/aml-screening/
Ongoing Monitoring	The four Art 26 clocks, including event-driven refresh and the Art 26(4) sanctions verification duty. shuftipro.com/ongoing-monitoring/
eIDV	Electronic identity verification where a qualifying eID route is available. shuftipro.com/eidv/

KEY RULE

AMLR's real test is whether identity, ownership, screening, monitoring and reporting behave as one connected record.

Where those functions sit with separate suppliers, officers reconcile them by hand, and the context needed to resolve an alert arrives late or not at all. The verified identity captured at onboarding should be the same record that screening, monitoring and reporting rely on for the life of the relationship.

**One glocal platform. The full compliance lifecycle, from sign-up to remediation.
Every industry, every region, every use case.**

NEXT STEP

Operationalising AMLR before July 2027?

Book a short call to map the Regulation against your onboarding stack.
shuftipro.com/request-demo/

Key legal and regulatory sources

01	Regulation (EU) 2024/1624 · AMLR	08	AMLA regulatory-instruments tracker
02	Directive (EU) 2024/1640 · AMLD6	09	AMLA CDD RTS consultation
03	Regulation (EU) 2024/1620 · AMLA	10	AMLA ongoing-monitoring consultation
04	Regulation (EU) 2023/1113 · TFR	11	European Commission · eIDAS framework
05	Directive (EU) 2015/849 · the repealed directive, for comparison	12	EU Trusted List Browser
06	Regulation (EU) 2024/1183 · eIDAS 2.0	13	EBA Remote Customer Onboarding Guidelines
07	Regulation (EU) No 910/2014 · eIDAS	14	European Commission · Impact assessment accompanying the AML package, SWD(2021) 190 final, 20 July 2021

Scope of this guide

This guide provides general regulatory information, not legal advice. Final AMLA measures, Member State rules, sector legislation and applicable sanctions should be assessed for the organisation's own circumstances. Draft Level 2 measures are identified as draft throughout and should be re-checked against the adopted text before implementation is closed.

Last reviewed 28 July 2026.



THE GLOBAL TRUST PLATFORM

One glocal platform. The full compliance lifecycle, from sign-up to remediation.

240+ countries and territories. 10,000+ document types actively verified each month. Every industry, every region, every use case.

[Book a Demo](#)

shuftipro.com
sales@shuftipro.com

