



# EU AML FRAMEWORK 2025

**AML**  
ANTI MONEY LAUNDERING

Regulatory Compliance Consulting

AML and ESG Operations

Risk Management

# TABLE OF CONTENT



## 01

### NEW REGULATORY FRAMEWORK

---

NEW FRAMEWORK OVERVIEW

AMLAR

AMLD6

WTR

AMLR

ACTION PLAN

## 02

### CONTACT

---

# New Regulatory Framework

The EU's new AML Package represents a comprehensive overhaul of the bloc's regulatory framework to combat money laundering and terrorist financing. Adopted in response to persistent vulnerabilities in the financial system and growing cross-border risks, this ambitious package aims to harmonize rules across Member States, improve enforcement, and strengthen cooperation among regulatory bodies.

By establishing a unified and risk-based approach, the EU AML Package seeks to close regulatory gaps, enhance transparency, and ensure robust defenses against financial crime. These measures reflect the EU's commitment to fostering trust, integrity, and resilience in its financial system while adapting to evolving global threats.

## Key components of the package include:

- › **AMLD 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.
- › **AMLR:** 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.
- › **AMLAR:** 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.
- › **WTR:** Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849



# New Framework Overview

## AMLD6

Date of entry into force : 10 July 2024  
Date of application: 10 July 2025  
[except for provisions related to access to UBO register for which date of application is 10 July 2026]

### The 6th Directive on AML/CFT

- › Transposition in national law is required; deadline is 10 July 2027 for most of the provisions
- › Contains provisions regarding national registers: UBO, bank account and real estate registers
- › Details the powers of national FIUs to receive and analyze STRs/SARs
- › Arranges the powers of national AML/CFT supervisors

## AMLAR

Date of entry into force : 1 July 2024  
Date of application: 1 July 2025

### The New AML Authority Establishment Regulation

- › Direct supervision of a selected number of financial institutions and crypto-asset service providers with high ML/TF risk
- › Indirect supervision through the coordination and oversight of national AML/CTF supervisors
- › Coordination and support mechanism for Financial Intelligence Unit (FIUs)

## AMLR

Date of entry into force : 10 July 2024  
Date of application: 10 July 2025

### The AML Single Rulebook

- › Direct applicability as of 10 July 2027 (limited exceptions); no transposition through national legislation required
- › Determines the scope of the AML/CTF policy in the EU
- › Strengthens and harmonizes the EU's AML/CFT material requirements, e.g. on CDD, PEP, UBO, reporting, record keeping, outsourcing, information sharing, etc.

## WTR

Date of entry into force : 1 June 2023  
Date of application: 30 December 2024

### Revision of the Fund Transfer Regulation

- › Extension of scope to include crypto-asset transfers
- › New obligations for crypto-asset service providers
- › Information of the sender and beneficiary of crypto-asset transfers inclusion with all transfers of crypto-assets

# AMLD6

Date of entry into force : 10 July 2024

Date of application: 10 July 2025

[except for provisions related to access to UBO register for which date of application is 10 July 2026]

## AMLD 6 establishes rules that require transposition at the national level on the following issues:

- › National and Supra-national ML/TF Risk Assessment: Conducted every four years by the EU Commission and each Member State.
- › Beneficial Ownership Register: Ensuring access for competent authorities and public persons.
- › Centralized Systems: Facilitating access to bank account and real estate ownership information.
- › Expansion of Financial Intelligence Units (FIUs): Direct access to a wide range of information and powers to suspend a business transaction or alert obliged entities of information relevant for the performance of customer due diligence.
- › AML Supervision: Adequate and effective supervision at national and cross-border level.
- › Cooperation Among Competent Authorities: Enhancing collaboration and information sharing.

## What does it mean for business?

Although the AMLD ensures that Member States establish the necessary infrastructure and mechanisms at the national level, it indirectly impacts institutions by:

- › Defining how authorities supervise and enforce the AMLR.
- › Requiring obliged entities to comply with more standardized processes for cross-border reporting and information-sharing.
- › Prompting institutions to tailor their risk management systems to align with national-level risk factors.
- › Obliging entities to navigate national-specific requirements that supplement the AMLR, such as access to centralized bank account or real estate registries

# AMLR

Date of entry into force : 10 July 2024

Date of application: 10 July 2025

## Obligated Entities

Art. 2, 3

## Supervision

Art. 81-84

- Areas in which the AMLA issues implementing technical standards or guidelines or prepares draft regulatory technical standards (RTS) and submits them to the Commission for adoption .

- Organization  
Art. 8, 11-18
  - Outsourcing  
Art. 18
- General Reporting Obligations  
Art. 14 / Art. 69-74

## Governance Arrangements

## 3rd Line

Internal Controls ●  
Art. 9

- Risk Assessment  
Art. 10
- High-Risk Third Countries  
Art. 29 / Art. 34 Sec. 1, 4
- Sanctions Compliance  
Art. 10, 20, 33-41
- SAR  
Art. 69-74
- Transaction Monitoring  
Art. 26

## 2nd Line

## 1st Line

CDD ●  
Art. 22, 26, 34, 41

Beneficial Ownership  
Chapter IV Art. 51-68

PEP ●  
Art. 2 Sec. 34-36 / Art. 42-46

Cash Payments  
Art. 19, 80

Information Sharing  
Art. 75-78



## What does it mean for business?

The AMLR expands the scope of AML compliance by including new categories of entities, establishes requirements for the governance structure that obliged entities must implement, and outlines how competent authorities, in collaboration, may supervise those entities.

### Governance Arrangements

- › **Organization:**  
Implementation of internal organizational obligations related to compliance with AML-R.
- › **Outsourcing:**  
Enhanced reporting and monitoring obligations, along with stricter restrictions on outsourcing activities.
- › **General Reporting:**  
Enhanced reporting and monitoring obligations, along with stricter restrictions on outsourcing activities.

### 3rd Line

- › **Internal Controls:**  
Obligation to implement robust control mechanisms ensuring adherence to internal AML guidelines and regulations.



## What does it mean for business?

### Risk Assessment:

- › Introduction of a mandatory minimum catalogue of risk factors for AML compliance.
- › Business-wide risk assessment is a must and as an extension of the previous scope, the risk of non-implementation and circumvention of targeted financial sanctions.

### High-Risk Third Countries :

- › Occasional transactions and business relationships with high-risk third countries are subject to EDD.

### Sanction Compliance:

- › Obligation to align with targeted financial sanctions as an integral component of risk management.
- › The responsibility lies with the MLRO, who is the point of contact for the competent authority.

### Suspicious Activity Reporting (SAR):

- › New special reporting obligations for identifying and reporting suspicious activities.
- › Requests for information from the FIU must be answered within five working days; the deadline may be shortened to less than 24 hours.
- › Credit and financial institutions providing services in relation to the purchase or transfer of ownership of certain high-value goods are obliged to report these transactions to the FIU.

### Transaction Monitoring:

- › Requirement for more frequent and systematic updates to customer data varying between 1-5 years in the context of the ongoing monitoring.





## What does it mean for business?

### Customer Due Diligence (CDD):

- › Stricter requirements for conducting customer due diligence processes like EDD for owners or applicants of Golden Passport and lower threshold for high-risk “high net worth individuals” when handling their assets by financial institutions, credit institutions and trusts.

### Beneficial Ownership:

- › Lowering the threshold for identifying beneficial ownership to a maximum of 15% in high-risk sectors.
- › Layered ownership and control structures should be thoroughly investigated.
- › The economic owners must not only be identified, but also verified.
- › All non-EU foreign entities that own real estate in the EU shall be registered retroactively to January 1, 2014.

### Politically Exposed Persons (PEP):

- › Broader definition of what constitutes a politically exposed person.
- › Siblings of heads of state, heads of government, ministers, deputy ministers and secretaries of state are now included as family members of PEP

### Cash Payments:

- › Introduction of an EU-wide upper limit of 10,000 € for cash transactions, coupled with new identification requirements for occasional cash payment of at least EUR 3,000 .

### Information Sharing:

- › Establishment of a legal framework to facilitate the exchange of information during customer due diligence.

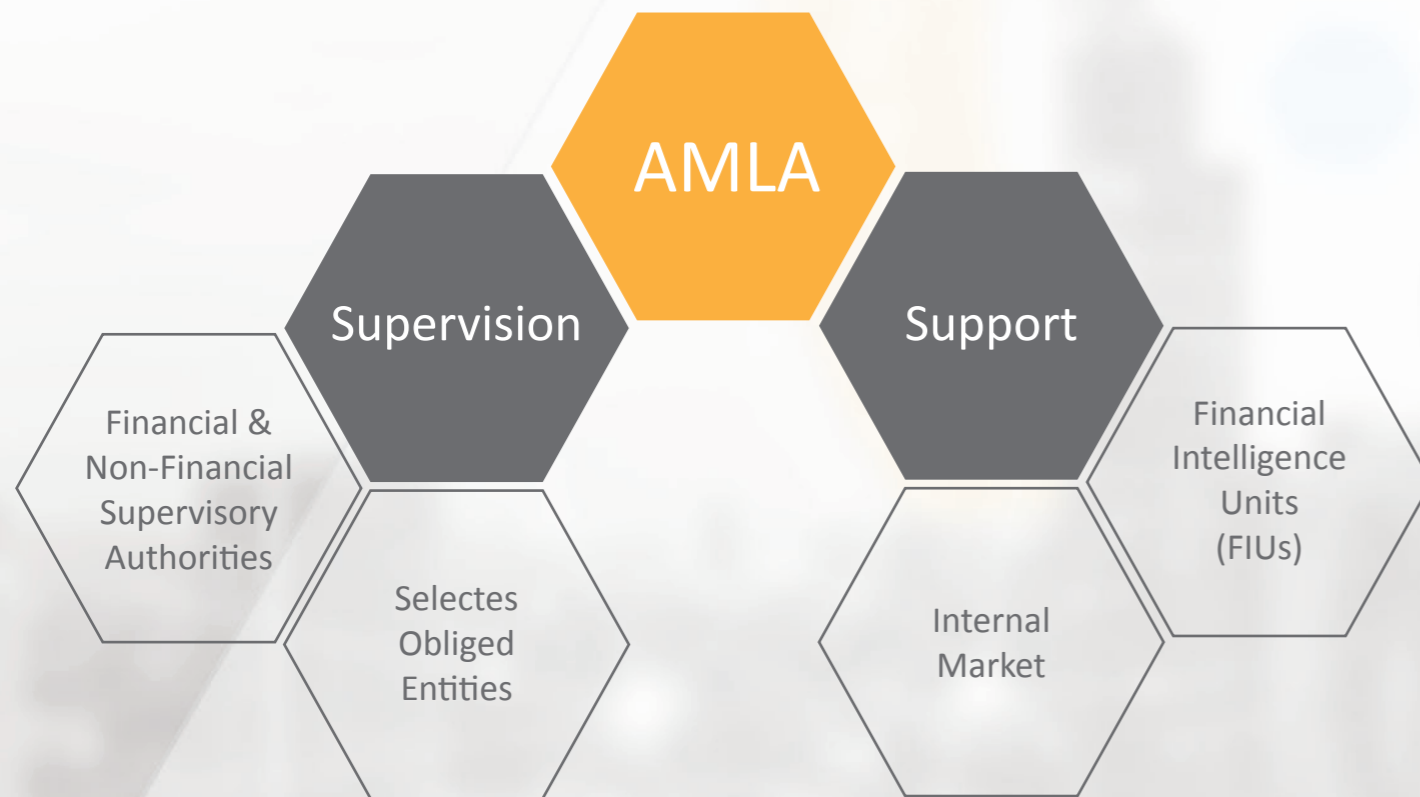
# AMLAR

Date of entry into force : 1 July 2024

Date of application: 1 July 2025

The **Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLAR)** is a decentralized EU agency that will coordinate national authorities to ensure the correct and consistent application of EU rules.

AMLAR has two primary responsibilities: **Supervision and Support**.



## What does it mean for business?

- › AMLAR will directly supervise up to 40 financial institutions deemed to pose the highest risk of money laundering or terrorist financing, including at least one institution from each EU member state.
  - › The methodology for classifying inherent and residual risk profiles will be established by AMLAR in at least 11 categories of obliged entities
  - › If the method does not select an obligated party from a respective member state, AMLAR will carry out an additional selection procedure together with the supervisory authorities
- › AMLAR will issue several Regulatory Technical Standards (RTS) and Guidelines to supplement the AMLD and AMLR. These publications will provide detailed instructions and practical guidance on compliance obligations. Obligated entities must closely monitor these releases and align their processes accordingly, as they clarify the specific measures and actions required to ensure full compliance.
- › To support the market, AMLAR will provide information and analysis on ML/TF risks. Institutions are expected to utilize this insight to develop a risk-based approach and optimize their AML frameworks
- › AMLAR has the authority to restrict activities, mandate changes in management structures, and propose the suspension of authorizations if violations of regulations are identified.

# When to Expect Regulatory Technical Standards

Regulatory Technical Standard (RTS) are legally binding standards and provide detailed technical rules to operationalize the regulation. They will be drafted by AMLA and formally adopted by the European Commission. Once adopted, they apply directly across the EU without the need for further national implementation.

## December 27th, 2025

Central AML/CFT database (art. 11(6) AMLA))

## January 1st, 2026

Risk assessment methodology to identify high risk credit institutions and financial institutions for direct supervision (art. 12(7) AMLA))

## July 10th, 2026

- › The minimum requirements of group-wide policies, procedures and controls, including minimum standards for information sharing within the group (art. 16(4) AMLA)
- › The minimum requirements for branches and subsidiaries in a less AML/CFT strict third countries (art. 17(3) AMLA)
- › CDD risk indicators (art. 19(9) AMLA)
- › Standard, simplified and enhanced due diligence (art. 28(1) AMLA)
- › Relevance and selection criteria for MS involvement in STRs (art. 69(3) AMLD)
- › The benchmarks and a methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency of risk profile review (art. 40(2) AMLD)
- › Central contact point (art. 41 (2) AMLD)
- › Duties of home and host supervisors (art. 46 (4) AMLD)
- › AML/CFT supervisory colleges in the financial sector (art. 49 (14) AMLD)
- › AML/CFT supervisory colleges in the non-financial sector (art. 50 (13) AMLD)
- › Breaches and pecuniary sanctions (art. 53 (10) AMLD)

# When to Expect Guidelines

Guidelines are non-binding instruments will be issued by AMLA to promote consistent practices and clarify expectations under EU AML laws. They provide recommendations, best practices, or interpretations of existing rules.

## July 10th, 2026

AMLA to publish guidelines on:

- › Risk and complexity elements to define the extent of Internal policies, procedures and controls (art. 9(4) AMLR)
- › Business wide risk assessment (art. 10(4) AMLR)
- › Risk factors / variables for new business relationship (art. 20(3) AMLR)
- › Ongoing monitoring (art. 26(5) AMLR)
- › Base amount for pecuniary sanctions (art. 53(11) AMLD)

## July 10th, 2027

AMLA to publish guidelines on:

- › Outsourcing relationship (art. 18(8) AMLR)
- › Compliance with AML rules and Payments Accounts Directive for credit institutions and financial institutions – jointly with European Banking Authority (EBA) (art. 21(4) AMLR)
- › ML/TF risks, trends and methods (art. 32(1) AMLR)
- › EDD measures for high-risk high-net-worth individuals for credit institutions, financial institutions and trust or company service providers (art. 34(5) AMLR)
- › EDD measures taken by crypto-asset service providers (art. 37(3) AMLR)
- › Self-hosted address related identifications and verifications (art. 40(2) AMLR)
- › PEPs risks and close associates (art. 42(2) AMLR)
- › Reliance on another obliged entities (art. 50 AMLR)
- › Indicators of suspicious activity or behaviors (art. 69(5) AMLR)

## July 10th, 2028

AMLA to publish guidelines on:

- › FIUs governance and tasks (art. 19(10) AMLD)
- › FIUs forwarding and receiving reports (art. 31(4) AMLD)
- › Risk-based approach to supervision (art. 40(3) AMLD)

## July 10th, 2029

AMLA to publish guidelines on:

- › Fit & properness Criteria (art. 6(8) AMLD)
- › Cooperation in relation to credit institutions or financial institutions (art. 64(6) AMLD)
- › Cooperation among competent authorities in supervision of obliged entities (art. 69 AMLD)

The WTR applies to transfers of funds sent or received by a payment service provider or an intermediary payment service provider established in the European Union.

The latest amendments under the new EU regulatory framework extend its scope to include transfers in crypto-assets, aiming to enhance the traceability of information accompanying transfers of funds and thereby support the prevention, detection, and investigation of money laundering and terrorist financing.

## What does it mean for business?

- › The payment service provider of the payer is responsible for ensuring the adequate recording of required information, while the payment service provider of the payee must verify the completeness of the information received.
- › Article 4 specifies the information that must be recorded and transmitted with each transfer, with requirements varying based on whether the transfer occurs within, from, or to the European Union.
- › The intermediary payment service provider must ensure that all information about the payer and payee is retained and included with the transfer.

## Conduct a Comprehensive Gap Analysis

- › Evaluate existing policies and procedures against current regulatory requirements alongside the development of guidelines by AMLA.
- › Identify gaps, inefficiencies, and areas requiring improvement.
- › Ensure the analysis is multi-purpose, addressing both regulatory compliance and operational efficiency.

## Define Priorities and Develop a Detailed Plan

- › Based on the Gap Analysis, distinguish areas for adjustments and improvements.
- › Outline a step-by-step roadmap, including specific tasks, required resources, and realistic timelines.

## Key Action Areas

- › Review and Update Policies and Procedures: Ensure alignment with updated regulations and operational best practices.
- › Upgrade IT Infrastructure: Implement technology solutions to support enhanced compliance, monitoring, and reporting.
- › Train Employees: Develop and deliver targeted training programs to equip staff with the knowledge and skills needed for the changes.
- › Monitor Implementation: Establish mechanisms for continuous oversight, ensuring that new measures are effectively adopted and deliver the desired outcomes.

## Implementation Oversight and Continuous Improvement

- › Regularly review progress against the plan and make necessary adjustments.
- › Monitor compliance, operational efficiency, and staff engagement during the implementation process.
- › Conduct periodic assessments to ensure sustained alignment with regulatory requirements.

# CONTACT

WIACON - Winde Analytics & Consulting GmbH  
Auenhainer Str. 35  
04463 Großpösna  
[www.wiacon.de/en](http://www.wiacon.de/en)



Andreas Winde

· MANAGING DIRECTOR ·

[andreas.winde@wiacon.de](mailto:andreas.winde@wiacon.de)

[LinkedIn-Profile](#)



Sophie Winde

· MANAGING DIRECTOR ·

[sophie.winde@wiacon.de](mailto:sophie.winde@wiacon.de)

[LinkedIn-Profile](#)