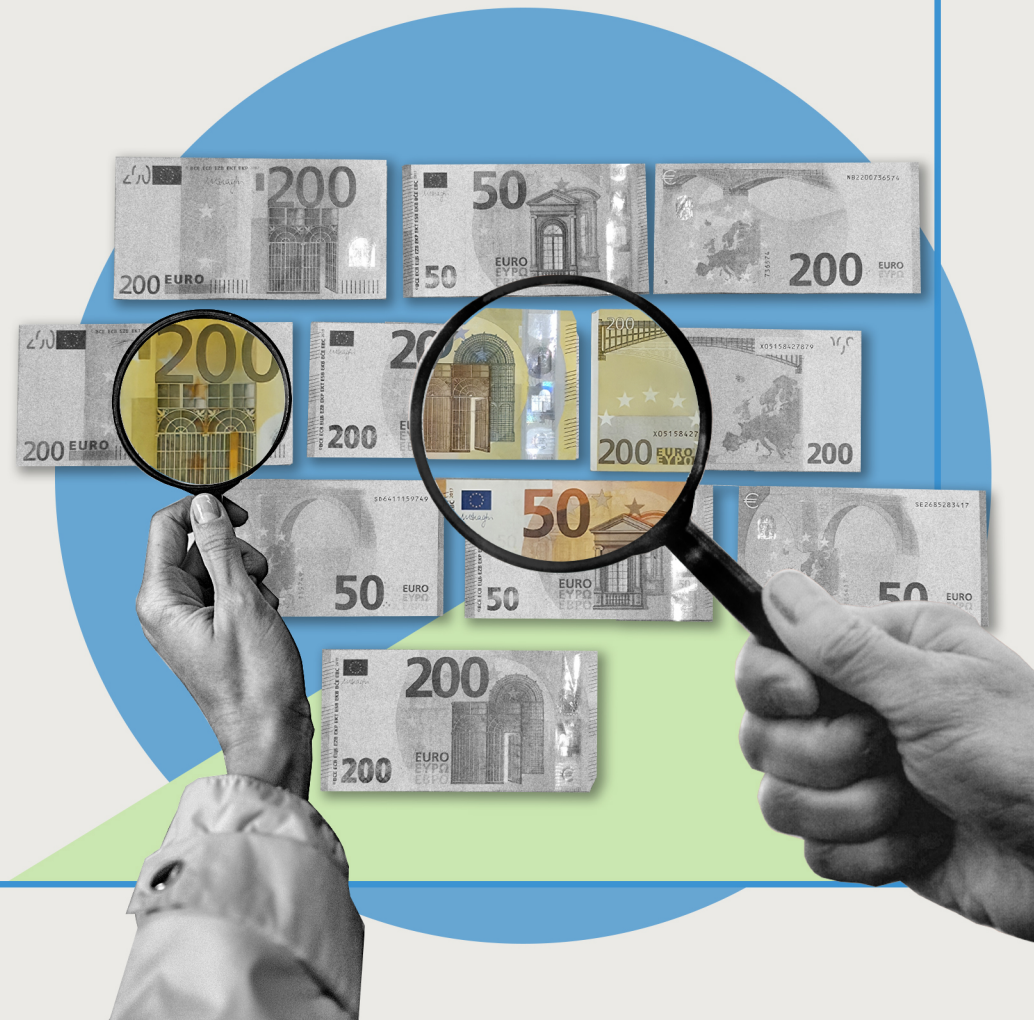


European Union legislative framework on Financial Intelligence Units (FIUs)

March 2026



ABOUT THIS SERIES OF EXPLANATORY DOCUMENTS

This document forms part of a series of five thematic legislative assessments covering crypto-assets, real estate, beneficial ownership, Financial Intelligence Units (FIUs), and obliged entities. The series has been prepared by Transparency International EU at the request of BIRN Albania and provides an overview of key developments introduced under the European Union's AML (Anti-Money Laundering) package adopted in 2024. It presents the original legal provisions which are accompanied by an explainers and examples of good practices identified by Transparency International through its reports, with the aim of supporting better understanding and implementation.

This is the original English version of the comparative analysis. To promote inclusive and informed engagement, the documents have also been translated into Albanian ([Link](#)). These translations are intended to support civil society organizations, academic institutions, investigative journalists, and other stakeholders in participating effectively in consultations and reform processes related to transparency and financial integrity.

These documents are intended for informational and analytical purposes only. They do not constitute legal advice, nor do they represent an official interpretation of European Union law.

SUMMARY OF THE EU AML INSTITUTIONAL FRAMEWORK: FINANCIAL INTELLIGENCE UNITS (FIUs)

The EU has developed a comprehensive institutional framework to address money laundering and terrorist financing risks through an integrated supervisory and intelligence system.

With the adoption of the [Sixth Anti-Money Laundering Regulation](#) (AMLR6), Financial Intelligence Units (FIUs) are formally classified as competent authorities, ensuring that all subsequent legal powers and data-access rights apply directly to them. The Regulation integrates the private sector into this intelligence pipeline by requiring obliged entities to report suspicious transactions promptly and unfiltered to their national FIU. It establishes a zero-threshold reporting rule and prohibits the outsourcing of final reporting decisions to third parties, thereby ensuring a direct and accountable relationship between the regulated sector and financial intelligence research.

The [Sixth Anti-Money Laundering Directive](#) (AMLD6) complements this framework by requiring each Member States to establish a single central national unit that is operationally independent and autonomous. To ensure the integrity of financial investigations, the sources state that FIUs must remain free from any undue political, government, or industry influence and possess the authority to take autonomous decisions on the analysis and dissemination of information. Furthermore, AMLD6 grants FIUs immediate and direct access to a broad range of data, including bank account registers, tax records, and law enforcement databases; this allows an effective mapping of criminal networks without procedural delays. Finally, the [AMLA Regulation](#) establishes the Anti-Money Laundering Authority as a central decentralized agency designed to add a crucial supervisory and intelligence dimension to the Union's internal defences. AMLA will coordinate national authorities to ensure the consistent application of AML rules and is expected to be fully operational in 2028, at which point it will begin the direct supervision of 40 selected high-risk entities. It will further serve as the technical hub for the network by hosting FIU.net, the secure platform for cross-border information exchange.

The AML package facilitates a reciprocal intelligence bridge between FIUs and other Union bodies, such as the European Public Prosecutor's Office (EPPO) and the European Anti-Fraud Office (OLAF), to support the prosecution of crimes affecting the Union's financial interests. To facilitate cooperation and the exchange of information in the field of law enforcement and judicial cooperation, AMLA is empowered to conclude working arrangements with various Union institutions, decentralized agencies, and other bodies. Taken together, these instruments create a multi-layered architecture intended to tackle corruption-related anti-money laundering cases before they reach trial.

AML REGULATION, “THE SINGLE REGULATORY FRAMEWORK”

RELEVANT LEGISLATION

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31st May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (known as the “single rulebook”)

PROVISIONS	EXPLAINER
Definitions Article 2	The article provides the legal definitions necessary for understanding the AML package. By classifying the FIU as a “competent authority”, the Regulation ensures that all subsequent powers and data-access rights granted to authorities apply directly to the FIUs.
1)For the purposes of this Regulation, the following definitions apply: (...) (44) ‘competent authorities’ means: (a) a Financial Intelligence Unit (FIU)	

<p>Compliance functions Article 11</p>	<p>This article mandates the appointment of a specific individual within each entity who acts as contact point with the FIU, ensuring that intelligence is not only gathered but is transmitted by a person with a “sufficiently high hierarchical standing”.</p>
<p>1) Obligated entities shall appoint one member of the management body (...) who shall be responsible for ensuring compliance with this Regulation.</p> <p>2) (...) The compliance officer shall (...) be responsible for reporting suspicious transactions to the FIU in accordance with Article 69(6).</p>	<p>This provision ensures that the FIU’s intelligence reach extends across complex corporate structures. It requires parent undertakings to implement group-wide policies that mandate the sharing of suspicious transaction reports and their underlying analyses between branches, ensuring that once a suspicion is flagged to an FIU, the entire group is aware, and the intelligence is utilised to manage risk across jurisdictions.</p>
<p>Group-wide requirements Article 16</p>	<p>3) (...) obliged entities within the group [shall be required] to exchange information where such sharing is relevant for (...) money laundering and terrorist financing risk management. The sharing of information (...) shall cover the identity and characteristics of the customer, its beneficial owners or the person on behalf of whom the customer acts, the nature and purpose of the business relationship and of the occasional transactions and the suspicions, accompanied by the underlying analyses, that funds are the proceeds of criminal activity or are related to terrorist financing reported to FIU pursuant to Article 69, unless otherwise instructed by the FIU.</p>

<p>Outsourcing Article 18</p>	
<p>1) Obligated entities may outsource tasks resulting from this Regulation to service providers. (...)</p> <p>3) (...) The following tasks shall not be outsourced under any circumstances: (...)</p> <p>(e) the reporting to FIU of suspicious activities (...) except, where such activities are outsourced to another obligated entity belonging to the same group and established in the same Member State.</p>	<p>This article creates a strict legal boundary for the FIU's reporting pipeline. It prohibits the delegation of the final decision to report a suspicion to an outside third party, ensuring that the legal responsibility and the direct relationship with the FIU remains within the regulated sector, thereby preventing the dilution of accountability in the transmission of financial intelligence.</p>
<p>Inability to comply with the requirement to apply customer due diligence Article 21</p>	
<p>Where an obliged entity is unable to comply with the requirement to apply customer due diligence measures (...) it shall refrain from carrying out a transaction or establishing a business relationship and shall terminate the business relationship and consider reporting a suspicious transaction to the FIU in relation to the customer.</p>	<p>This provision identifies a failure in the gatekeeper vetting process as a primary intelligence trigger. It mandates that if an entity cannot verify who a customer is or what they are doing, it must not only stop the business but also evaluate if that lack of transparency constitutes a suspicion that must be reported to the FIU, effectively turning a compliance failure into a source of intelligence for the unit.</p>
<p>Scope of application of enhanced due diligence measures Article 34</p>	
<p>3) (...) obliged entities shall take into account (...) any other indicators of higher risk such as notifications issued by the FIU.</p>	<p>If a FIU identifies specific threats or emerging patterns and issues a formal notification, obliged entities are legally required to integrate this intelligence into their risk assessments. This notification serves as a mandatory indicator of higher risk, compelling the entity to apply enhanced due diligence measures to manage and mitigate the risks specifically identified by the national authorities.</p>

<p>Reporting obligations Chapter V</p>	<p>Chapter V identifies reporting obligations for FIUs.</p>
<p>Article 69</p> <p>1) Obligated entities (...) shall cooperate fully with the FIU by promptly:</p> <p>(a) reporting to the FIU (...) [and] responding to request by the FIU for additional information (...).</p> <p>(b) (...) FIUs may shorten that deadline (...) to less than 24 hours.</p> <p>Article 70</p> <p>1) (...) The designated self-regulatory body shall forward the information referred to [the FIU] (...) promptly and unfiltered.</p>	<p>Article 69 represents the central mandate for the FIU's work by requiring prompt transmission of financial intelligence from the private sector to the state. It establishes a “zero-threshold” reporting rule, meaning that a suspicion must be reported regardless of the monetary value or sum of money involved; there is no minimum financial limit that must be reached before an entity is required to alter the FIU. Beyond the financial report, the FIU is granted extensive powers to demand follow-up data, including transaction records, within strict timeframes.</p> <p>Article 70 ensures the FIU still receives ‘unfiltered’ data even when reported via a professional body for sensitive sectors.</p>
<p>Refraining from carrying out transactions Article 71</p>	
<p>1) Obligated entities shall refrain from carrying out transactions (...) until they have submitted a report (...) and have complied with any further specific instructions from the FIU.</p>	<p>Obligated entities must report suspicious transactions for a three-day FIU review period, unless immediate execution is necessary to avoid ‘tipping off’ the suspect.</p>
<p>Disclosure to FIU Article 72</p>	
<p>Disclosure of information to the FIU in good faith (...) shall not involve the obliged entity (...) in liability of any kind.</p>	<p>The article establishes a liability exemption for those who report to the FIU ensuring that individuals and institutions can fulfil their reporting obligations without fear or legal retaliation.</p>

<p>Threshold-based reports of transactions in certain high-value goods Article 74</p>	<p>This provision imposes a reporting obligation to persons trading in high-value goods, credit institutions and financial institutions towards the FIU in the deadlines imposed by the FIU.</p>
<p>1) Persons trading in high-value goods shall report to the FIU all transactions involving the sale of [motor vehicles, watercraft, and aircraft] (...). 3) Reporting (...) shall be carried out within the deadlines imposed by the FIU</p>	<p>This provision ensures that while information can flow between private entities to combat financial crime, the FIU remains the ultimate authority and gatekeeper of that intelligence.</p>
<p>Exchange of information in the framework of partnerships for information sharing Article 75</p>	<p>This provision ensures that while information can flow between private entities to combat financial crime, the FIU remains the ultimate authority and gatekeeper of that intelligence.</p>
<p>1) Obligated entities intending to participate in a partnership for information sharing shall notify their respective supervisory authorities (...). Where relevant, the supervisory authority shall also consult the FIUs.</p> <p>(...) 4) (k) the sharing of information on suspicious transactions (...) shall only take place where the FIU to which the suspicious transactions report was submitted (...) has agreed with such disclosure.</p> <p>5) Information received in the context of a partnership for information sharing shall not be further transmitted, except where:</p> <p>(b) the information is to be included in a report submitted to the FIU or provided in response to a FIU request (...).</p>	<p>This provision ensures that while information can flow between private entities to combat financial crime, the FIU remains the ultimate authority and gatekeeper of that intelligence.</p>

Data protection and record retention

Chapter VII

Article 77

1) **Obligated entities shall retain** the following documents and information:

(b) a record of the assessment undertaken (...) including the **information** and circumstances considered and the results of such assessment, whether or not such assessments **results in a suspicious transaction report being made to the FIU.**

Article 78

Obligated entities shall have systems in place that enable them to **respond fully and speedily to enquiries from the FIU.**

These articles focus on the FIU's need for retrospective intelligence. **Article 77** mandates that entities keep physical or digital evidence of the interaction with the FIU for 5 years while **Article 78** complements this by requiring entities to maintain technical systems that allow the FIU to map out the financial footprint of a suspect across different institutions in a full and speed manner.

<p>Limits to large cash payments in exchange for good or services Article 80</p>	
<p>4) (...) Payments or deposits (...) above the limits shall be reported to the FIU within the deadlines imposed by the FIU.</p>	<p>This article requires banks to report high-value cash movements so the FIU can analyse the source and patterns of physical currency regardless of an initial suspicion.</p>
<p>Cooperation between FIUs and the EPPO Section 1</p>	
<p>Article 81</p> <p>Each FIU shall without undue delay report to the EPPO the results of its analyses and any additional relevant information where there is reasonable ground to suspect that money laundering and other criminal activity (...) of which the EPPO could exercise its competence.</p> <p>Article 82</p> <p>FIU and the EPPO may exchange the results of strategic analyses</p>	<p>These articles create a reciprocal intelligence bridge between the FIU and the EPPO. It ensures that FIU financial analysis support EU-level prosecutions of crimes like fraud or corruption, while allowing the FIU to pull investigative information from the EPPO to strengthen its own national analyses.</p>

Cooperation between FIUs and OLAF

Section 2

Article 83

1) (...) **Each FIU shall transmit** without undue delay the **results of its analyses (...) to OLAF** where there are reasonable grounds to suspect that fraud, corruption or any other illegal activity affecting the Union's financial interests (...) in respect of which OLAF could exercise its competence (...).

3) **FIUs and OLAF may exchange** the results of strategic analyses

Article 84

OLAF shall respond in a timely manner to requests for information by an FIU.

Similar to the EPPQ, these provisions establish a direct line of communication between FIUs and OLAF.

Reports

Article 88

(...) The Commission shall submit reports (...) assessing the necessity and proportionality of (...) introducing **harmonised format for the reporting of transactions based on the usefulness of those reports for the FIUs.**

The Commissions must verify whether the automatic 'threshold reports' generated by the private sector are actually providing useful intelligence for the FIUs in their mission to detect and combat money laundering.

THE SIXTH AML DIRECTIVE

RELEVANT LEGISLATION

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 (known as the AMLD6)

PROVISIONS	EXPLAINER
Establishment of FIUs Article 19	
<p>1) Member States shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing (...)</p> <p>2) The FIU shall be the single central national unit responsible for receiving and analysing reports submitted by obliged (...).</p> <p>3) The FIU shall be responsible for disseminating the results of its analyses and any additional information to relevant competent authorities where there are grounds to suspect money laundering, its predicate offences or terrorist financing. It shall be able to obtain additional information from obliged entities.</p> <p>4) Each FIU shall be operationally independent and autonomous, which means that it shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decision to analyse, request and, (...), disseminate specific information. It shall be free from any undue political, government or industry influence or interference.</p>	<p>This article establishes the FIU as the national hub for financial intelligence, centralizing reports from obliged entities, customs authorities and supervisors. To ensure the integrity of investigations, the FIU must possess the capacity to take autonomous decisions regarding the analysis and dissemination of information. Even if the FIU is located within the structure of another authority (such as Ministry of Finance or Police), its core functions must be operationally separated from other functions of that host body.</p> <p>The FIU's mandate is split in two distinct analytical streams:</p> <ul style="list-style-type: none">- Operational analysis, which focuses on individual cases and specific targets- Strategic analysis, which identifies broader money laundering/terrorist financing trends and patterns.

Member States are legally required to provide adequate resources to allow the FIU to deploy assets independently. Staff must be held to high professional standards, including the ethical handling of big data sets and strict procedures to manage conflicts of interest. Furthermore, the FIU must designate a Fundamental Rights Officer. (see Article 20 on Fundamental Rights Officer).

AMLD5 vs AMLD6

Compared to AMLD5, AMLD6 provides stronger legal safeguards for the integrity of FIUs by explicitly establishing their operational independence and autonomy.

Good practices

In some countries, **FIUs are integrated directly within national law enforcement authorities, making cooperation seamless**. In **Portugal and Lithuania**, FIU sits within the judicial of financial police, a structure, investigators view as a major advantage for transitioning intelligence into active cases. Similarly, **Italy** leverages strong institutional synergies and specialised financial police to ensure that suspicious transaction reports lead to effective prosecutions. These countries minimise coordination delays and ensure that high-value financial data is prioritised for investigation.

<p>Access to information Article 21</p>	<p>FIUs are granted direct access to a broad range of data, including bank account registers (see Article 16 of AMLD6), tax records, customs data, and law enforcement databases. Access is considered 'direct and immediate' when obtained via automated mechanisms without intermediaries. This comprehensive access is intended to allow FIUs to map out complex criminal networks effectively without being impeded by the involvement of other authorities.</p>
<p>1) Member States shall ensure that FIUs (...) have access to the information that they require to fulfil their tasks, including financial, administrative and law enforcement information (...) [including] at least:</p> <p>(a) immediate and direct access to (...) financial information (...); [and]</p> <p>(b) immediate and direct access to (...) administrative information (...).</p>	<p>AML5 vs AML6</p> <p>AML6 removes national discrepancies and ensures FIUs across the EU have the same analytical tools. In AML5 the specific lists of accessible data were not fully harmonised.</p>
<p>Responses to requests for information Article 22</p>	<p>This article establishes the FIU as a central information hub for other domestic competent authorities (such as law enforcement authorities and tax authorities). It ensures that intelligence already held by the FIU can be shared to support specific cases but crucially maintains the FIU's operational autonomy.</p> <p>Moreover, it mandates a reciprocal relationship where receiving authorities must report back on how the intelligence was used, creating feedback loop that refines the FIU's future analytical accuracy.</p>
<p>1) Member States shall ensure that FIUs are able to respond in a timely manner to reasoned requests for information (...) by the competent authorities (...) in their respective Member States where that information is already held by the FIU and is necessary on a case-by-case. The decision on conducting the dissemination of information shall remain with the FIU.</p> <p>Where there are objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses (...) the FIU shall not be obliged to comply with the request for information. In such cases, the FIU shall provide the reasons in writing to the requesting authority.</p> <p>2) Competent authorities shall provide feedback (...) to allow the FIU to improve its operational analysis function.</p>	<p>AML5 vs AML6</p> <p>AML6 introduces more structured requirements for domestic cooperation. Unlike AML5, it explicitly requires receiving authorities to provide feedback to the FIU to improve its future operational analysis.</p>

<p>Provisions of information to supervisors Article 23</p>	<p>For risk-based supervision to be effective, supervisors need to know which 'gatekeepers' (e.g., banks) are failing in their duties. This article requires the FIU to share intelligence on the reporting performance of these entities.</p>
<p>1) (...) FIU provide supervisors, spontaneously or upon request, information that may be relevant for the purposes of supervision (...), including (...)</p> <p>(a) the quality and quantity of suspicious transactions reports submitted by obliged entities;</p> <p>(b) the quality and timelines of responses provided to FIU requests (...);</p> <p>(c) relevant results of strategic analyses.</p>	<p>AMLD5 vs AMLD6</p> <p>AMLD6 significantly improves oversight by replacing the generalised cooperation of AMLD5 with a mandatory, exhaustive list of performance data the FIU must share with supervisors.</p>
<p>Suspension or withholding of consent Article 24</p>	<p>These preventive powers allow the FIU to restrain criminal funds before they are moved or hidden. Because this affects property rights, the Article sets strict timelines to ensure the action is legally proportionate while allowing the FIU to confirm suspicions and refer the case for seizure.</p>
<p>1) Member States shall ensure that FIUs are empowered to take urgent actions (...) to suspend or withhold consent to that transaction. (...) Member States shall lay down the period of suspension (...) which shall not exceed 10 working days. (...) FIU is empowered to take urgent action (...) to suspend the use of that account (...) which shall not exceed 5 working days.</p>	<p>AMLD5 vs AMLD6</p> <p>AMLD6 improves the framework by harmonizing maximum suspension timelines across the EU, eliminating the national discrepancies that existed under AMLD5.</p>
<p>Instructions to monitor transactions or activities Article 25</p>	<p>This provision shifts the FIU into a proactive investigative role, gaining additional insights into a high-risk subject's financial behaviour over time. Real-time monitoring helps detect sophisticated patterns that a single report might miss, facilitating more effective analysis and potential account suspension.</p>
<p>Member States shall ensure that FIUs are empowered to instruct obliged entities to monitor (...) the transactions or activities (...) for persons who present a significant risk.</p>	

<p>Alerts to obliged entities Article 26</p>	<p>The FIU provides targeted intelligence to the private sector to improve their customer due diligence procedures. By alerting entities to specific high-risk persons or regions, the FIU ensures that 'gatekeepers' are updated on emerging threats and can adjust their risk management systems accordingly.</p>
<p>Member States shall ensure that FIUs are able to alert obliged entities of information relevant for the performance of customer due diligence (...)</p> <p>(a) type of transactions (...) that present a significant risk;</p> <p>(b) specific persons (...);</p> <p>(c) specific geographic areas.</p>	
<p>FIU annual report Article 27</p>	<p>//</p>
<p>Each Member State shall ensure that its FIU publishes an annual report on its activities</p>	
<p>Feedback by FIU Article 28</p>	<p>Feedback is the primary tool for quality control, helping the private sector refine its ability to detect and report suspicious activities. By evaluating the quality and timing of reports, the FIU ensures that incoming intelligence is actionable.</p>
<p>1) Member States shall ensure that FIUs provide obliged entities with feedback on the reporting of suspicious (...). Such feedback shall cover at least the quality of the information provided, the timeliness of reporting (...). The FIU shall provide feedback at least once per year. (...)</p> <p>FIUS shall report on annual basis to AMLA on the provision of feedback to obliged entities (...). By 10 July 2028, AMLA shall issue recommendations to FIUs on best practices and approaches towards the provision of feedback.</p> <p>2) Member States shall ensure that FIUs provide customs authorities with feedback (...)</p>	<p>AMLD5 vs AMLD6</p> <p>AMLD6 improves the reporting mechanism by making feedback a mandatory legal obligation to be performed at least annually where AMLD5 only required it 'if available'.</p>

<p>Cooperation between FIUs Article 29</p>	<p>Because illicit money frequently is transnational, national barriers must not hinder the capacity to develop preventive analyses. This article ensures that irrespective of whether an FIU is administrative, judicial or law enforcement-based, it is legally obligated to assist its counterparts. It treats the Union as a single intelligence zone rather than a collection of individual national systems.</p>
<p>Member States shall ensure that FIUs cooperate to the greatest extent possible, regardless of their organisational status</p>	
<p>Protected channels of communication Article 30</p>	<p>Secure infrastructure is a prerequisite for trust. The Directive formalises FIU.net as the encrypted system for cross-border cooperation, managed by AMLA to ensure high technological standards and uniform data protection. The platform allows FIUs to match their data with other units in a pseudonymous manner on a hit/no-hit basis to identify links between financial information and criminal intelligence.</p>
<p>1) A system for the exchange of information between FIUs of Member States (FIUs.net) shall be set up. FIU.net shall ensure the secure communication and exchange of information (...) [and] shall be managed by AMLA</p>	<p>AMLD5 vs AMLD6</p> <p>AMLD6 formalise FIU.net and the centralised management by AMLA providing a more technical stability and advanced features like the hit/no-hit mechanism.</p>

Exchange of information between FIUs

Article 31

1) Member States shall ensure that FIUs **exchange (...)** any **information that may be relevant (...)** regardless of the type of predicate offences that may be involved, and even if not identified at the time of the exchange.

Speed is critical in countering money laundering. This article sets strict **time limits for responses** (generally 5 working days, or 1 working day in urgent cases) to meet the procedural constraints of investigations. It ensures that information flows freely even if the specific underlying crime (e.g., fraud or drug trafficking) has not been proven yet and requires requested FIUs to use their full range of domestic powers to assist.

AMLD5 vs AMLD6

AMLD6 sets timelines on the exchange of information to improve cross-border cooperation.

Good practices

AMLA will facilitate the work of FIUs by providing advanced IT and artificial intelligence services that significantly enhance their data analysis and detection capabilities. By offering a secure, centralized hub for information exchange and coordinating joint analysis.

<p>Joint analyses Article 32</p>	<p>FIUs are empowered to conduct integrated operational analyses through joint teams assisted by AMLA. These teams pool resources and information to obtain a full picture of anomalous cross-border activities that a single national authority could not see alone.</p>
<p>1) Member States shall ensure that their FIUs are able to carry out joint analysis (...) [and]</p> <p>2) set up a joint analysis team for a specific purpose and limited period.</p>	<p>Good practices</p> <p>In 2023, the French and Luxembourg FIUs demonstrated a successful joint analysis to dismantle a transnational VAT fraud network. Moving beyond traditional request-based information sharing, the two FIUs cross-referenced extensive datasets (including bank record and tax data) via secure channels (e.g., FIU.net) to map out a complex web of shell companies and financial flows that would have been invisible to a single jurisdiction. This synergy allowed them to gain a comprehensive view of the criminal infrastructure, resulting in a direct case referral to the European Public Prosecutor's office (EPPO).¹</p>
<p>Use by FIUs of information exchanged between them Article 33</p>	<p>Data received from other FIUs must be used strictly for statutory tasks. To maintain mutual trust, the transmitting unit has the right to set specific conditions to ensure intelligence is used only for the purposes for which it was provided.</p>

¹ Transparency France International, *Case study: How do financial intelligence units cooperate with each other?* (15 October 2025), accessed [09/02/2026], <https://transparency-france.org/2025/10/15/combating-money-laundering-focus-on-the-alcba-a-best-practice-in-international-cooperation/>

<p>Consent to further dissemination of information exchanged between FIUs Article 34</p>	<p>A receiving FIU must obtain permission from the original providing unit before sharing data with another authority (such as the police). Consent should be granted promptly and to the largest extent possible in exceptional cases.</p>
<p>1) (...) Dissemination of [exchanged] information by the receiving FIU to any other authority (...) is made subject to the prior consent by the FIU providing the information.</p>	
<p>Effect of criminal law provisions Article 35</p>	<p>Legal inconsistencies between Member States regarding the definition of underlying crimes must not be used to block assistance. An FIU cannot refuse to cooperate simply because its domestic definition of a crime differs from that of the requesting country. This ensures a harmonised defensive front across the internal market.</p>
<p>Differences between national law definitions of predicate offences shall not impede the ability of FIUs to provide assistance to another FIU and shall not limit the exchange, dissemination and use of information.</p>	
<p>Confidentiality of reporting Article 36</p>	<p>Member States must protect the identity of “gatekeepers” (such as bank employees) who flag suspicious activities. FIUs are prohibited from disclosing the source of a report when disseminating findings to investigators to prevent retaliation and ensure the reporting mechanism remains effective.</p>
<p>1) Member States shall ensure FIUs have in place mechanisms to protect the identity of the obliged entities and their employees (...) who report suspicions (...)</p> <p>2) FIUs do not disclose the source of the report.</p>	<p>AMLD5 vs AMLD6</p> <p>AMLD6 adds a layer of protection for gatekeepers by ensuring their identity is shielded during the investigative phase.</p>

AMLA REGULATION

RELEVANT LEGISLATION

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 Regulation (EU) No 1094/2010 and (EU) No 1095/2010 (known as the AMLA Regulation)

PROVISIONS	EXPLAINER
Establishment and scope of action Article 1	
<p>1) The Authority for Anti-Money Laundering and Countering the Financing of Terrorism ('The Authority') is hereby established.</p> <p>(...)</p> <p>3) The objective of the Authority shall be to protect the public interest, the stability and integrity of the Union's financial system, and the proper functioning of the internal market by (...):</p> <p>(a) preventing the use of the Union's financial system for the purposes of money-laundering and terrorist financing;</p> <p>(b) contributing to the identification and assessment of ML/TF risks and threats across the internal market</p> <p>(c) ensuring high quality supervision in the area of (...) AML/CFT across the internal market;</p> <p>(e) contributing to the harmonisation of practices in the detection of suspicious transactions or activities by FIUs;</p> <p>(f) supporting and coordinating the exchange between FIUs, and between FIUs and other competent authorities.</p>	<p>The AMLA is a Union agency with legal personality established to serve as the central pillar of an integrated EU-wide AML/CFT supervisory and intelligence system. Its headquarters is in Frankfurt, Germany.</p> <p>The main objectives of AMLA are moving beyond fragmented national implementation of AML package to ensure the proper functioning of the internal market. Its mandate includes identifying external and internal threats, establishing a harmonised supervisory methodology, and acting as a support and coordination mechanism for national FIUs to ensure consistent detection of suspicious activities.</p> <p>While the AMLA Regulation entered into force in 2024, most of its provisions became applicable from 1 July 2025, while foundational articles started to apply from 26 June 2024 to allow for the initial establishment of the Authority. The Commission remained responsible for the Authority's initial operations until 31 December 2025. The AMLA is to start its full activities by the beginning of 2027.</p>

Tasks

Article 5

- 5) The Authority shall perform the following tasks with respect to FIUs (...):
- (a) maintain an up-to-date list of FIUs within the Union;
 - (b) **monitor changes in the legal framework of FIUs**, as well as in their organisation, (...)
 - (c) **support the work of FIUs** and contribute to improved cooperation and coordination between FIUs;
 - (d) **contribute to the identification and the selection of relevant cases for the conduct of joint analyses by FIUs**;
 - (e) develop appropriate methods and procedures for the conduct of joint analyses by FIUs of cross-border cases;
 - (f) **set up, coordinate, organise and facilitate the conduct of joint analyses** carried out by FIUs;
 - (g) provide assistance to FIUs, (...)
 - (h) **conduct peer reviews** of the activities of FIUs (...)
 - (i) **develop and make available to FIUs tools** and services to enhance their analyses capabilities (...)
 - (j) **develop, share and promote expert knowledge** on detection, analysis, and dissemination methods of suspicious transactions;
 - (k) at the request of FIUs, provide them with specialised **training and assistance**, (...)
 - (l) support, at the request of FIUs, their interaction with obliged entities by providing expert knowledge to obliged entities
 - (m) **prepare and coordinate assessments and strategic analyses of ML/TF threats**, risks and methods identified by FIUs

This provision establishes the AMLA as the central operational hub and service provider for the Union's FIUs network. Its objective is to move beyond insufficient effective cooperation for cross-border cases by creating an integrated system that ensures effective cooperation. The AMLA is mandated to provide the technical backbone for this system by hosting FIU.net, which facilitates the secure exchange of information and data. Beyond technical support, the AMLA takes a leadership role in joint analysis, allowing it to directly coordinate investigations into cross-border cases that units might struggle to handle alone. The task of conducting strategic analyses and peer reviews ensures the harmonisation of practices in the detection of suspicious transactions. This allows the AMLA to identify ML/TF risks and promote the exchange of best practices and training activities to ensure all FIUs function at a consistently high level of quality.

<p>Powers of the Authority Article 6</p>	<p>These powers allow the AMLA to gather the high-level data and statistics needed to identify Union-wide risks while providing the legal means to direct and process data for specific collaborative investigations.</p>
<p>3) With respect to FIUs in Member States, the Authority shall have the following powers:</p> <p>(a) to request non-operational data and analyses (...) for the assessment of threats (...);</p> <p>(b) to collect information and statistics</p> <p>(c) to obtain and process information and data required for initiating, conducting and coordinating joint analyses</p> <p>(d) to issue guidelines and recommendations</p>	
<p>AML/CFT supervisory methodology Article 8</p>	<p>This provision establishes a critical feedback loop between intelligence and supervision. It mandates that the harmonised methodology used to oversee financial institutions must be continuously informed by actual criminal patterns, risks, and threats detected by national FIUs and law enforcement. By incorporating this intelligence, the Regulation ensures that supervisory practices remain risk-based and responsive to the latest methods of ML/TF identified on the ground.</p>
<p>4) (...) The Authority shall periodically review and update its supervisory methodology, taking into account the evolution of risks affecting the internal market, including risks and threats identified by national law enforcement authorities and FIUs.</p>	
<p>Cooperation between the Authority and FIUs Article 39</p>	<p>This article creates a formal legal obligation for national FIUs and the AMLA to work together, establishing a structured mechanism where cooperation is a mandatory duty rather than a voluntary arrangement.</p>
<p>1) The Authority shall be responsible for ensuring the effective and consistent cooperation between FIUs within the framework of the support and coordination mechanism for FIUs. (...)</p> <p>2) The Authority and FIUs shall be subject to a duty of cooperation in good faith, (...) and to an obligation to exchange information that is necessary to fulfil their respective tasks.</p> <p>3) (...) An FIU may inform the Authority in the case of a failure by another FIU to cooperate. In that case, the Authority shall act as a mediator.</p>	

Conduct of joint analysis

Article 40

3) Where (...) an FIU of a Member States identifies a potential need to conduct a joint analysis with one or several FIUs in other Member States, it shall notify the Authority thereof. (...) Where **the Authority** assesses that the case is relevant, it **shall**, within five days of the initial notification, **inform FIUs** in all relevant Member States and invite them to take part in the joint analysis. (...) **FIUs** in all relevant Member States **shall consider taking part** in the joint analysis.

4) If at least one other FIU agrees to take part in the joint analysis, the Authority shall ensure that the analysis is launched within 20 days of the initial assessment (...).

5) Any **FIU that declines to participate** in the conduct of the joint analysis **shall provide the reasons** (...). The Authority shall provide such explanation without delay to the FIU that identified the need for a joint analysis.

6) Upon the express consent of all FIUs participating in the joint analysis, (...) the **Authority** supporting the joint analysis **shall be granted access to all data** (...). Where an FIU refuses to grant access to the (...) Authority, (...) it shall ensure that the information is otherwise provided (...). Where several FIUs refuse to grant access to the data (...), the Authority shall re-assess whether the tasks that its staff would perform justify its support. (...)

8) **Upon the express consent of all FIUs participating** (...) the **Authority** (...) **shall be authorised to cross-match, on the basis of a hit-no hit system, the data of those FIUs with the data made available by other FIUs and Union bodies, offices and agencies within their respective mandates.** (...) In the case of a hit, the Authority shall share with all FIUs participating in the joint analysis the information that triggered the hit (...).

The article establishes a structured Union framework for cross-border financial investigations. The Regulation imposes strict deadlines (e.g., 5 days to notify FIUs) to ensure that intelligence is processed while it is still actionable.

FIUs refusing to participate in joint analysis must provide written reasons, providing a layer of transparency and preventing barriers to cooperation.

The hit-no hit system is an information-sharing mechanism used primarily in LEAS and administrative databases to determine if information on a specific person or object exists in another system without immediately revealing the full, sensitive details. It is a privacy-preserving tool designed to foster cooperation while maintaining data protection standards. It can be used as well to avoid overlapping investigations and duplicate procedures. In the context of AMLA it allows to cross-match pseudonymized data against records held by others FIUs or Union bodies. As mentioned in recitals 45, this allows investigators to establish in real time if a subject is known in another jurisdiction without unnecessary processing of personal data. Only when a 'hit' occurs is the specific information that triggered the match shared, ensuring that deep data exchange is targeted, proportionate, and strictly limited to what is necessary for the conduct of the joint analysis.

Request by the Authority for the initiation of a joint analysis

Article 42

- 1) When the **Authority** identifies a potential need to conduct a joint analysis (...) it **shall inform the concerned FIUs** thereof and request them to take part in the joint analysis.
- 2) The concerned FIUs shall inform the Authority without undue delay, making best efforts to do so within five days of receipt of the request, of their decision (...)
- 3) Where an FIU requested to take part in the joint analysis refuses a request made by the Authority (...) it shall inform the authority of the reasons for its decision without undue delay, making best efforts to do so within five days of receipt of the request.

This article grants the AMLA a proactive role in identifying cross-border cases that require collective action. While the AMLA cannot force participation, it can officially request it. The requirement for national units to provide formal reasons for refusal ensures transparency and discourages arbitrary non-cooperation in complex investigations affecting multiple jurisdictions.

Review of the methods, and procedures for, and conduct of, joint analysis

Article 43

- 2) **FIUs** that participated or were otherwise involved in a joint analysis **may provide their feedback to the Authority** on the **conduct of the analysis**, including feedback on the **operational support** provided by the Authority (...) as well as feedback on the **outcome of the analysis**, the **methods** and **procedures** in place (...), the **tools** available and the coordination between the participating FIUs (...)
- 3) (...) **On the basis of the feedback** (...) or on its own initiative, the **Authority may issue a follow-up report**. (...) The follow-up report shall be **shared with all FIUs** (...). The conclusions and recommendations (...) shall be shared with all FIUs that participated in the joint analysis (...) insofar as those (...) do not contain confidential or restricted information.

This provision establishes a continuous improvement mechanism for Union-level intelligence operations. By mandating a feedback loop between the AMLA and participating national units, the Regulation ensures that the methods for joint analysis stay effective against evolving criminal threats. The resulting follow-up reports serve to identify and share best practices across all Union FIUs without compromising the confidentiality of specific cases.

National FIU delegates

Article 44

- 1) **The FIU of each Member State shall delegate one or more staff members** to the Authority (...)
- 2) **FIU delegates shall have** the status of staff of the delegating FIU (...) [and] be granted, (...) **access to the Authority's data and information.**
- 4) FIU delegates shall be granted **access to any data accessible by their delegating FIU** (...).
- 6) The Executive Board shall determine the rights and obligations of FIU delegate in relation to the Authority.

This provision mandates a physical presence of national experts at the AMLA's premises. These delegated staff act as a bridge, retaining access to their home country's databases to support the AMLA's union-wide analysis and coordination tasks.

Mutual assistance in the area of cooperation between FIUs

Article 45

- 1) In the context of promoting cooperation between, and supporting the work of, FIUs, the **Authority**, taking into account the needs of FIUs, **shall promote common approaches, methods and best practices.** The Authority shall also organise and facilitate in particular the following activities:
 - (a) **training programmes**, including with respect to technological innovation;
 - (b) **personnel exchange** and secondment schemes;
 - (c) **exchanges of practices** between FIUs
 - (d) development or procurement of **IT tools**;
- 2) An FIU may submit to the Authority a request for assistance related to the tasks of the FIU (...)
- 3) The Authority shall make every effort to provide the requested assistance, including by considering the support to be provided with its own human resources as well as coordinating and facilitating the provision of any form of assistance by other FIUs on a voluntary basis.

This article goes beyond simple cooperation; it creates a mutual assistance framework where individual units can request operational or personnel support.

<p>Mediation between FIUs Article 46</p>	
<p>1) The Authority may facilitate a solution in the case of a disagreement between two or more FIUs regarding individual cases related to cooperation, including the exchange of information (...). The purpose of such mediation shall be to reconcile divergent points of view between the FIUs and to adopt a non-binding opinion.</p> <p>2) Where a disagreement cannot be solved by direct contact and dialogue between the FIUs concerned, the Authority shall launch a mediation procedure upon the request of one or more of those FIUs.</p>	<p>This provision introduces a structured mediation mechanism to resolve operational conflicts that could impede the flow of financial intelligence across the Union. When national units cannot resolve a dispute regarding information sharing or case cooperation through direct dialogue, AMLA intervenes to provide a neutral forum for reconciliation. The Regulation ensures accountability by requiring the involved units to report back within three months on how they have addressed the mediation findings, ensuring that operational disagreements are formally tracked and managed at Union level.</p>
<p>FIU.net Article 47</p>	
<p>1) The Authority shall ensure adequate, uninterrupted and secure hosting of FIU.net, and ensure the management, maintenance and development of FIU.net.</p>	<p>The Regulation assigns the AMLA the technical responsibility for FIU.net to ensure it uses updated technology, while strictly limiting the AMLA's access to private communications between national units.</p>
<p>Peer review Article 48</p>	
<p>The Authority shall set up a peer review process of the activities of FIUs (...)</p>	<p>The peer review process objectively assesses whether national units have the independence, staff, and IT security required to function effectively within the Union framework.</p>

General Board
Section 1 (Chapter III)

Article 57

- 1) The General Board shall have either the supervisory composition (...) or the FIU composition (...)
- 3) The General Board in FIU composition shall be composed of: (...)
 - (b) the heads of FIUs, with the right to vote

Article 58

- 4) The General Board in FIU composition shall establish a standing committee (...) to support performing its tasks (...) including by submitting proposals and preparing draft decisions.

Article 59

- 1) (...) the members of the General Board (...) in FIU composition shall act as a whole and shall neither seek nor take instructions from Union institutions (...) nor from any government.

Article 60

- 3) The General Board in FIU composition shall perform the tasks and adopt the decisions referred to in Article 5(5) and Chapter II, Section 6.

The General Board is the AMLA's primary decision-making body responsible for adopting harmonized rules and coordination policies. To ensure specialised expertise, it is divided in two:

- **General Board in supervisory composition:** with the Chair and heads of national supervisors for oversight matters
- **General Board in FIU composition:** with the Chair and Head of national FIUS for financial intelligence coordination. The Board is supported by a standing committee of 9 FIU experts who prepare technical draft decisions.

All members must act with absolute independence, prioritising Union interests over any external or government instructions

<p>Accountability and reporting Article 84</p>	<p>This Article ensures that AMLA is accountable to Union institutions for the performance of its duties. To maintain transparency, it must publish annual reports and share record of its high-level meetings. However, to protect the integrity of FIUs, AMLA is prohibited from disclosing confidential FIU related data to ensure that reporting requirements do not jeopardize the security of ongoing investigation.</p>
<p>4) (...) The Authority shall (...) provide the European Parliament with a comprehensive and meaningful record of the proceedings of that meeting (...). Such record shall not reflect (...) FIU data-related, unless otherwise provided for in the legislative acts (...)</p>	<p>This Articles positions the AMLA as the central representative for the Union’s financial intelligence interests on the world stage. This includes providing specific support to the Egmont Groups which is the primary international network for information exchange between FIUs.</p>
<p>Cooperation with third countries and international organisations Article 95</p>	<p>This Articles positions the AMLA as the central representative for the Union’s financial intelligence interests on the world stage. This includes providing specific support to the Egmont Groups which is the primary international network for information exchange between FIUs.</p>
<p>1) (...) The Authority may develop contacts and enter into administrative arrangements with AML/CFT authorities in third countries that have regulatory supervisory and FIU-related competences (...) as well as with international organisations and third-country administrations.</p> <p>2) The Authority may develop model administrative arrangements (...) FIUs shall make every effort to follow such model arrangements.</p> <p>3) In cases where the interaction between (...) several Union supervisory authorities and FIUs with, (...) third-country authorities, concerns matter falling within the scope of the Authority’s tasks (...), the Authority shall have a leading role in facilitating such interaction where necessary.</p> <p>4) The Authority shall, (...) contribute to the united, common, consistent and effective representation of the Union’s interests in international fora (...) by supporting the work and objectives of the Egmont Groupe of Financial Intelligence Units.</p>	<p>This Articles positions the AMLA as the central representative for the Union’s financial intelligence interests on the world stage. This includes providing specific support to the Egmont Groups which is the primary international network for information exchange between FIUs.</p>

Evaluation and review

Article 102

1) By 31 December 2030, and **every five years** thereafter, the **Commission shall draw up report on the Authority's performance** (...). That report shall, in particular, address:

(c) the **impact of the activities** related to support and coordination of FIUs, and in particular the coordination of the joint analyses of cross-border activities and transactions conducted by FIUs.

2) The **report (...)** shall also examine whether:

(c) it is **appropriate to confer on the Authority additional tasks** in the area of support and coordination of the work of FIUs.

This article establishes a mandatory performance audit. The review is designed to be forward-looking; if the support and coordination mechanism proves successful, the Commission may recommend expanding the AMLA's mandate and powers.

ENDNOTES

- [Chasing Grand Corruption](#) includes author/editor information from the report's PDF header (Isabelle Bühchner as author).
- [The Transparency France International case study](#) is an online publication dated 15 October 2025.
- [European Parliament and Council of the European Union](#). 2024. 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. Official Journal of the European Union, OJ L 2024/1640, June 19.



Transparency International EU

31 Rue du Commerce, 1000 Brussels

<http://www.transparency.eu/>

+32 (0) 4 97 49 90 81

brussels@transparency.org

Transparency Register ID: 501222919
71