TRANSPARENCY INTERNATIONAL EU

European Union's legislative framework on virtual assets: crypto

February 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 LEGAL FRAMEWORK ON VIRTUAL ASSET: CRYPTO

The European Union has developed a comprehensive regulatory framework to address the money laundering and terrorist financing risks associated with crypto-assets. At its core, the MiCA Regulation provides the first EU-wide legal framework on services related to crypto-assets that are not already covered by existing EU financial services legislation. It introduces a clear classification of crypto-assets into asset-referenced tokens (ARTs), e-money tokens (EMTs) and other crypto-assets. It establishes uniform rules on transparency, disclosure, consumer protection, market integrity and prudential requirements for crypto-asset service providers (CASPs). All CASPs operating in the Union must be authorised to do so (MiCA license). They are subject to ongoing supervision by national competent authorities, and must comply with conduct-of-business, governance, and market-abuse rules. Issuers of significant ARTs and EMTs fall under the direct supervision of the European Banking Authority (EBA).

With the adoption of the latest EU AML package in 2024, CASPs are fully integrated in the AML/CFT framework. They are now classified as obliged entities, subject to customer due diligence, transaction monitoring, reporting obligations and enhanced controls for high-risk activities, including transfers involving self-hosted wallets. The Transfer of Funds Regulation extends the travel rule, originally for traditional payments, to crypto-assets, ensuring full traceability within the EU. Moreover, the AML framework is reinforced at institutional level with the newly established Anti-Money Laundering Authority which will directly supervise a limited number of high-risk, cross-border obliged entities, including CASPs.

The Digital Operational Resilience Act, known as DORA, complements this framework by ensuring that the European financial sector can withstand, respond to, and recover from all types of ICT-related disruptions and threats. MiCA-authorised CASPs and issuers of asset-referenced tokens are subject to stringent requirements on ICT risk management, incident reporting, operational resilience testing and oversight of third-party ICT providers, thereby mitigating cyber and operational risks inherent in crypto-asset markets.

Finally, crypto-asset activities are brought within the scope of EU tax transparency rules through the DAC8 Directive, which amends the Directive on administrative cooperation in the field of taxation. It requires CASPs to collect and report detailed information on crypto-asset transactions and users. It also mandates the automatic exchange of that information between Member States' tax authorities. This mechanism enables national tax authorities to detect cross-border crypto and capital gains to prevent tax evasion.

Taken together, these instruments create a multi-layered EU framework aimed at increasing transparency, traceability and supervisory convergence while strengthening market integrity and mitigating money-laundering risks linked to crypto-assets.

MICA REGULATION (REGULATION ON MARKETS IN CRYPTO-ASSETS)

RELEVANT LEGISLATION

Regulation of 31 May 2023 on markets in crypto-assets (known as the MiCA Regulation)

Fully applicable since 30 December 2024

PROVISIONS	EXPLAINER
Subject matter Article 1	The Regulation establishes **harmonised rules for crypto-assets at EU level**.
1) This Regulation lays down uniform requirements for the **offer to the public and admission to trading on a trading platform** of **crypto-assets** other than asset-referenced tokens and e-money tokens, of asset-referenced tokens and of e-money tokens, as well as requirements for crypto-asset service providers.	Objectives: 1) Provide a legal framework for crypto-assets not covered by existing EU legislation on financial services; 2) Support innovation, promote crypto-assets and the wider use of distributed ledger technology (DLT); 3) Secure an appropriate level of consumer and investor protection and market integrity; 4) Enhance financial stability.

Scope Article 2	
1) This Regulation applies to **natural and legal persons** and certain **other undertakings** that are engaged in the **issuance, offer to the public and admission to trading of crypto-assets** or that **provide services related to crypto-assets in the Union.** 2) Exceptions (…)	//
Asset classification **Material scope** Article 3	
Three types of crypto assets: 1) Asset-referenced token (ART) → more under Title III 2) Electronic money token (EMT) → more under Title IV 3) Other crypto-assets not covered under points 1 or 2 → Title II, Articles 4 to 15	The Regulation covers three types of crypto assets (as defined in Article 3(1)(5)): 1) ART: means a type of crypto-asset that is not an electronic money token and that purports to **maintain a stable value by referencing another value or right or a combination thereof**, including one or more official currencies; 2) EMT: means a type of crypto-asset that purports to **maintain a stable value by referencing the value of one official currency**; 3) Other crypto-assets If it is a **financial instrument** (stock/bond), it falls under MiFID II, as opposed to MiCA.

White Paper Obligations Articles 4-15	
1) A crypto-asset white paper shall contain all of the following information, as further specified in Annex I: (a) **information about the offeror or the person seeking admission to trading**; (…) c) **information about the operator of the trading platform** in cases where it draws up the crypto-asset white paper; (…) (e) **information about the offer to the public of the crypto-asset** or its admission to trading; (f) information about the crypto-asset; (…) (j) information on the principal **adverse impacts on the climate and other environment-related adverse impacts** (…). 2) All of the information listed in paragraph 1 shall be **fair, clear and not misleading**. The crypto-asset white paper shall not contain material omissions and shall be presented in a **concise and comprehensible form**. (…) 10) The crypto-asset white paper shall be made available in a **machine-readable format**.	The offeror, or the issuer, if different from the offeror, must draw up, notify to the competent authority of their home Member State, and publish on their website, which must be publicly accessible, a **Crypto-Asset White Paper** as well the **marketing communications**, if any, in respect of that crypto-asset. The crypto-asset white papers and, where applicable, the marketing communications, must remain **available on the website of the offerors for as long as the crypto-assets are held by the public**. An offeror that provides **information** that is not **complete, fair, or clear**, or that is misleading, will be **liable** to a holder of the crypto-asset for any loss incurred due to that infringement.

Right of Withdrawal Article 13	
1) Retail holders who purchase crypto-assets other than asset-referenced tokens and e-money tokens either directly from an offeror or from a crypto-asset service provider placing crypto-assets on behalf of that offeror shall have a **right of withdrawal**. Retail holders shall have a period of **14 calendar days** within which to withdraw from their agreement to purchase crypto-assets other than asset-referenced tokens and e-money tokens **without incurring any fees or costs and without being required to give reasons**. The period of withdrawal shall begin from the date of the agreement of the retail holder to purchase those crypto-assets. (…) 4) The right of withdrawal referred to in paragraph 1 shall **not apply where the crypto-assets have been admitted to trading prior to their purchase by the retail holder**.	Retail holders that acquire crypto-assets other than asset-referenced tokens or e-money tokens directly from the offeror, or from a crypto-asset service provider, should be provided with a **right of withdrawal during a period of 14 days after their acquisition**. The right of withdrawal should not apply where crypto-assets other than asset referenced tokens or e-money tokens are admitted to trading prior to the purchase by the retail holder because, in such a case, the price of such crypto-assets depends on the fluctuations of the markets in crypto-assets.
Reserve of Assets Article 36	
1) Issuers of **asset-referenced tokens** shall constitute and at all times maintain a reserve of assets. 2) The reserve of assets shall be **legally segregated from the issuers' estate**, as well as from the reserve of assets of other asset-referenced tokens, in the interests of the holders of asset-referenced tokens in accordance with applicable law, so that creditors of the issuers have no recourse to the reserve of assets, in particular in the event of insolvency. (…) 5) Issuers that offer two or more asset-referenced tokens to the public shall operate and **maintain segregated pools of reserves of assets for each asset-referenced token**.	In order to cover their liability against holders of asset-referenced tokens, issuers of asset-referenced tokens should constitute and maintain a reserve of assets matching the risks reflected in such liability. The reserve of assets should be used for the benefit of the holders of the asset-referenced tokens when the issuer is not able to fulfil its obligations towards the holders, such as in insolvency.

Authorisation of crypto-asset service providers Articles 59-65	
Article 59: 1) A person shall not provide crypto-asset services, within the Union, unless that person is: (a) a **legal person or other undertaking that has been authorised as crypto-asset service provider** in accordance with Article 63; or (b) a **credit institution, central securities depository, investment firm, market operator, electronic money institution, UCITS management company, or an alternative investment fund manager** that is allowed to provide crypto-asset services pursuant to Article 60. **Article 60:** 1) A credit institution may provide crypto-asset services if it notifies the information referred to in paragraph 7 to the competent authority of its home Member State at least 40 working days before providing those services for the first time. **Article 62:** 1) Legal persons or other undertakings that intend to provide crypto-asset services shall **submit their application for an authorisation as a crypto-asset service provider to the competent authority of their home Member State**. **Article 64:** Withdrawal of authorisation of a crypto-asset service provider **Article 65:** Cross-border provision of crypto-asset services	//

Obligations for all crypto-asset service providers Article 66-74	
1) Obligation to act honestly, fairly and professionally in the best interests of clients 2) Prudential requirements 3) Governance arrangements 4) Information to competent authorities 5) Safekeeping of client's crypto-asses and funds 6) Complaints-handling procedures 7) Identification, prevention, management and disclosure of conflict of interests 8) Outsourcing 9) Orderly wind-down of crypto-asset service providers	//
Environmental impact Article 66	
(5) Crypto-asset service providers shall make publicly available, in a prominent place on their website, information related to the **principal adverse impacts on the climate and other environment-related adverse impacts** (…). That information may be obtained from the crypto-asset white papers.	Transactions in crypto-assets might have adverse impacts on the climate. These should be adequately identified and disclosed by issuers of crypto-assets and crypto-asset service providers.

Market abuses Articles 86-92	
Title VI shall apply to acts carried out by any person concerning crypto-assets that are admitted to trading or in respect of which a request for admission to trading has been made. 1) Inside information 2) Public disclosure of inside information 3) Prohibition of insider dealing 4) Prohibition of unlawful disclosure of inside information 5) Prohibition of market manipulation 6) Prevention and detection of market abuse	Title VI contains a number of prohibitions aimed at preventing and prohibiting market abuse involving crypto-assets.
Supervision Title VII	
Article 93: 1) Member States shall designate the **competent authorities responsible for carrying out the functions and duties provided for in this Regulation**. Member States shall **notify those competent authorities to EBA and ESMA.** **Article 96:** 1) For the purposes of this Regulation, the competent authorities shall cooperate closely with ESMA (…) and with EBA (…). **Article 109:** 1) ESMA shall establish a register of: (a) crypto-asset white papers for crypto-assets other than asset-referenced tokens and e-money tokens; (b) issuers of asset-referenced tokens; (c) issuers of e-money tokens; and (d) crypto-asset service providers.	Competent authorities should be conferred with sufficient powers to supervise the issuance, offer to the public and admission to trading of crypto-assets, including asset-referenced tokens or e-money tokens, as well as to supervise crypto-asset service providers. Those powers should include the power to suspend or prohibit an offer to the public or an admission to trading of crypto-assets or the provision of a crypto-asset service, and to investigate infringements of the rules on market abuse.

Administrative penalties and other administrative measures by competent authorities Articles 111 to 116	
Article 111 1) (…) Member States shall, in accordance with national law, provide for **competent authorities** to have the power to take **appropriate administrative penalties** and other administrative measures (…): **Article 114** 1) A decision imposing administrative penalties and other administrative measures for an infringement of this Regulation in accordance with Article 111 shall be published by competent authorities on their official websites without undue delay after the natural or legal person subject to that decision has been informed of that decision. **Article 115** 1) The competent authority shall, on an annual basis, provide ESMA and EBA with aggregate information regarding all administrative penalties and other administrative measures imposed in accordance with Article 111. ESMA shall publish that information in an annual report.	When determining the type and level of an administrative penalty or other administrative measure, competent authorities should take into account all relevant circumstances, including the gravity and the duration of the infringement and whether it was committed intentionally.
Supervisory responsibilities of EBA Article 117	
1) Where an **asset-referenced token has been classified as significant** in accordance with Article 43 or 44, the issuer of such asset-referenced token shall carry out its activities under the supervision of EBA. (…) 4) Where an **e-money token issued by an electronic money institution has been classified as significant** in accordance with Article 56 or 57, EBA shall supervise the compliance of the issuer of such significant e-money token with Articles 55 and 58.	Given that EBA should be mandated with the **direct supervision** of issuers of **significant asset-referenced tokens** and of **significant e-money tokens**, (...), it is necessary to ensure that EBA is able to protect the public interest by contributing to the short, medium, and long-term stability and effectiveness of the financial system for the Union economy, its citizens and businesses.

DELEGATED REGULATIONS UNDER MICA

LEGISLATIVE TEXT	EXPLAINER
Commission Delegated Regulation (EU) 2024/1506 specifying certain criteria for classifying ARTs and EMTs as significant	The Delegated Regulation sets criteria used to classify Asset Reference Tokens" (ART) and "E-Money Tokens" (EMT) as significant ART and EMT issuers. The criteria set out in Article 43(1) of the MiCA Regulation for classifying asset-referenced tokens as **significant ARTs** apply also for the classification of **e-money tokens** as significant EMTs. To enable the **European Banking Authority (EBA)** to determine whether the activities of the issuer of the ARTs or EMTs are significant on an international scale, and whether ARTs or EMTs or their issuers are to be considered as interconnected with the financial system, the Delegated Regulation **distinguishes between core and ancillary indicators**.
Commission Delegated Regulation (EU) 2024/1507 specifying the criteria and factors to be taken into account by ESMA, the EBA, and competent authorities in relation to their intervention powers	The Delegated Regulation sets conditions for authorities exercising powers of intervention on products regulated by MiCA. It provides a **list of criteria and factors** to be taken into account by competent authorities**, ESMA and the EBA**, when there is a significant investor concern or threat to the orderly functioning and integrity of markets in crypto-assets or to the stability of the whole or part of the financial system of the Union or of at least one Member State.

Commission Delegated Regulation (EU) 2024/1504 specifying the procedural rules for the exercise of the power to impose fines or periodic penalty payments by the EBA on issuers of significant ARTs and issuers of significant EMTs	Rules governing EBA's sanctioning power. The **EBA's power to impose a periodic penalty payment** is to be exercised with due regard to the right to defence and is not to be maintained beyond the period necessary. Both the power to impose fines and periodic penalty payments and the power to enforce fines and periodic penalty payments should be **subject to a limitation period**. To ensure safekeeping of collected fines and periodic penalties, the EBA should deposit them on **interest-bearing accounts** that are opened exclusively for the purpose of a single fine or periodic penalty payments aiming at ending a single infringement.
Commission Delegated Regulation (EU) 2024/1503 specifying the fees charged by the EBA to issuers of significant ARTs and issuers of significant EMTs	An annual **supervisory fee** should be established to cover the actual and estimated costs to be incurred by the European Banking Authority (EBA) when performing supervisory tasks. The annual supervisory fees should be **adjusted** every year to match the estimated costs.

THE EU ANTI-MONEY LAUNDERING PACKAGE 2024

RELEVANT LEGISLATION

Regulation (EU) 2023/1113 of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets (TFR)
(known as the Transfer of Funds Regulation (TFR))

PROVISION	EXPLAINER
Subject matter Article 1	
This Regulation lays down rules on the information on (…) **on originators and beneficiaries accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing**, where at least one of the payment service providers or crypto-asset service providers involved in the transfer of funds or transfer of crypto-assets is established or has its registered office, as applicable, in the Union. In addition, this Regulation lays down rules on internal policies, procedures and controls to ensure implementation of restrictive measures where at least one of the payment service providers or crypto-asset service providers involved in the transfer of funds or transfer of crypto-assets is established or has its registered office, as applicable, in the Union.	**General introduction to the TFR** The revised Transfer of Funds Regulation (TFR) ensures that **crypto-asset transfers can be traced like traditional money transfers**. Anonymous crypto wallets are effectively banned, enhancing transparency and reducing misuse. Moreover, certain transfers of crypto-assets entail specific high-risk factors for money laundering, terrorist financing and other criminal activities, in particular transfers related to products, transactions or technologies designed to enhance anonymity, including privacy wallets, mixers or tumblers. The TFR extends the travel rule, originally for traditional payments, to crypto, requiring **every transfer to include full information on the sender and the receiver**, ensuring traceability across borders and preventing money laundering, terrorist financing, and other crimes. This aligns with FATF Recommendation 16 and complements the MiCA Regulation, which sets licensing and prudential rules for crypto-asset service providers.

Scope Article 2	
1) This Regulation shall also apply **to transfers of crypto- assets**, including transfers of crypto-assets executed by means of crypto-ATMs, where the crypto-asset service provider, or the intermediary crypto-asset service provider, of either the originator or the beneficiary **has its registered office in the Union**. (…) 4) This Regulation **shall not** apply to a transfer of crypto-assets where any of the following conditions is met: a) both the originator and the beneficiary are crypto-asset service providers acting on their own behalf; b) the transfer constitutes a person-to-person transfer of crypto-assets carried out without the involvement of a crypto- asset service provider.	EU crypto rules apply mainly to transfers involving EU-based service providers, except for transfers strictly between providers or direct peer-to-peer transfers.

Definitions Article 3	
(10) **'transfer of crypto-assets'** means any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same; (…) (14) **'crypto-asset'** means a crypto-asset as defined in Article 3(1), point (5), of Regulation (EU) 2023/1114, except where falling within the categories listed in Article 2(2), (3) and (4) of that Regulation or otherwise qualifying as funds; (15) **'crypto-asset service provider'** means a crypto-asset service provider as defined in Article 3(1), point (15), of Regulation (EU) 2023/1114, where performing one or more crypto-asset services as defined in Article 3(1), point (16), of that Regulation; (16) '**intermediary crypto-asset service provider'** means a crypto-asset service provider that is not the crypto-asset service provider of the originator or of the beneficiary (…); (19) '**crypto-asset account'** means an account held by a crypto-asset service provider in the name of one or more natural or legal persons and that can be used for the execution of transfers of crypto-assets;	//

Obligations on crypto-asset service provider of the originator Article 14	
The crypto-asset service provider of the **originator** shall ensure that transfers of crypto-assets are accompanied by the following information: • on the originator: (a) the name, (b) the beneficiary's distributed ledger address, (c) the beneficiary's crypto-asset account number, (d) the current LEI or, in its absence, any other available equivalent official identifier • on the beneficiary: (a) the name, (b) the beneficiary's distributed ledger address, (c) the beneficiary's crypto-asset account number, (d) the current LEI or, in its absence, any other available equivalent official identifier	**Article 3(1), point (15) of the MiCA Regulation** 'crypto-asset service provider' means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis (…).

Obligations on the crypto asset provider of the beneficiary
Articles 16-18

Article 16:
(1) The crypto-asset service provider of the **beneficiary** shall implement effective procedures, including, where appropriate, **monitoring after or during the transfers**, in order to detect whether the information referred to in Article 14(1) and (2) on the originator and the beneficiary is included in, or follows, the transfer or batch file transfer of crypto-assets.
(2) In the case of a transfer of crypto-assets made from a **self-hosted address**, the crypto-asset service provider of the beneficiary shall obtain and hold the information referred to in Article 14(1) and (2) and shall ensure that the transfer of crypto-assets can be individually identified.
Without prejudice to specific risk mitigating measures taken in accordance with Article 19b of Directive (EU) 2015/849, in the case of a transfer of an **amount exceeding EUR 1000 from a self-hosted address**, the crypto-asset service provider of the beneficiary shall take adequate measures to assess whether that address is owned or controlled by the beneficiary.
Article 17:
1) The crypto-asset service provider of the beneficiary shall **implement effective risk-based procedures**, (…), **for determining whether to execute, reject, return or suspend a transfer** of crypto-assets lacking the required complete information on the originator and the beneficiary and for taking the appropriate follow-up action.
(…)
2) **Where a crypto-asset service provider repeatedly fails to provide the required information on the originator or the beneficiary**, (…) it **shall report that failure**, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter-terrorist financing provisions.
Article 18:
The crypto-asset service provider of the beneficiary shall take into account missing or incomplete information on the originator or the beneficiary as a factor when assessing whether a transfer of crypto-assets, or any related transaction, is suspicious and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849.

Operational flow for exchanges under Articles 16-18 (travel rule compliant)

- Incoming transfer check
  - Verify if originator and beneficiary info is attached.
- Self-hosted wallet check
  - For transfers > €1,000, verify wallet ownership by the user.
- Verification before credit
  - Cross-check beneficiary info via reliable independent sources.
- Risk assessment
  - If info is missing: execute, reject, return, or suspend based on risk level.
- Request or reject
  - Ask originator/beneficiary for missing info, or reject/return funds if non-compliant.
  -
- Escalation for repeat offenders
  - Issue warnings → set deadlines → restrict or terminate relationship.
- Regulator reporting
  - Report non-compliance (risk-factor) to FIUs.

N.B.: in the case of a transfer of crypto- assets not registered on a network using DLT (..)/ from a crypto-asset account, and/or the transfer of crypto-assets made to self-hosted address, it should always be individually identified.

Obligations on intermediary crypto-asset service providers
Articles 19-22

Article 19:

Intermediary crypto-asset service providers shall ensure that all the information received on the originator and the beneficiary that accompanies a transfer of crypto-assets is transmitted with the transfer and that records of **such information are retained and made available on request to the competent authorities**.

Article 20:

The intermediary crypto-asset service provider shall implement effective procedures, including, where appropriate, monitoring after or during the transfers, in order to detect whether the information on the originator or the beneficiary (…), has been submitted previously, simultaneously or concurrently with the transfer or batch file transfer of crypto-assets, including where the transfer is made to or from a self-hosted address.

Article 21:

The intermediary crypto-asset service provider shall establish **effective risk-based procedures**, including risk-sensitive procedures under Article 13 of Directive (EU) 2015/849, to **determine whether to execute, reject, return, or suspend a transfer** lacking the required originator or beneficiary information, and to take appropriate follow-up action.

(…)

The intermediary shall report the failure and actions taken to the competent AML/CFT authority.

Article 22:

Same as Article 18 (for the beneficiary)

Summary of the obligations for the beneficiary and the intermediary

- Detection of missing information
  - The beneficiary CASP has a specific obligation to verify self-hosted addresses, including ownership checks for amounts over €1,000.
  - Intermediaries monitor missing info but don't have the self-hosted address ownership requirement.
- Handling missing or incomplete information is the same
- Retention of information
  - Explicit retention obligation is emphasized for intermediaries, while beneficiary CASPs have it implied.
- Reporting obligations are the same

Internal policies, procedures and controls to ensure implementation of restrictive measures Article 23	
Payment service providers and crypto-asset service providers shall have in **place internal policies, procedures and controls to ensure the implementation of Union** and national **restrictive measures** when performing transfers of funds and crypto-assets under this Regulation. The European Banking Authority (EBA) shall issue guidelines by 30 December 2024 specifying the measures referred to in this Article.	//

AML REGULATION, THE SINGLE REGULATORY FRAMEWORK

RELEVANT LEGISLATION

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** (known as the single rulebook)

PROVISIONS	EXPLAINER
Definitions Article 2	Objective: crypto-asset service providers are exposed to the misuse of new channels for the movement of illicit money. The scope of EU AML legislation has therefore been expanded to crypto-asset service providers**, to mitigate any risk of misuse of crypto-assets for money laundering or terrorist financing purposes**.
6) 'financial institution' means: (…) (i) **a crypto-asset service provider**; (…) 7) 'crypto-asset' means a crypto-asset as defined in Article 3(1), point (5), of Regulation (EU) 2023/1114 except when falling under the categories listed in Article 2(4) of that Regulation; 8) 'crypto-asset services' means crypto-asset services as defined in Article 3(1), point (16), of Regulation (EU) 2023/1114, with the exception of providing advice on crypto-assets as referred to in Article 3(1), point (16)(h), of that Regulation; 9) 'crypto-asset service provider' means a crypto-asset service provider as defined in Article 3(1), point (15), of Regulation (EU) 2023/1114 where performing one or more crypto-asset services; (…)	

23) ‘shell institution’ means: (…) (b) for crypto-asset service providers: an entity whose name appears in the register established by the European Securities and Markets Authority pursuant to Article 110 of Regulation (EU) 2023/1114 or third country entity providing crypto-asset services without being licensed or registered nor subject to AML/CFT supervision there; 24) ‘crypto-asset account’ means a crypto-asset account as defined in Article 3, point (19), of Regulation (EU) 2023/1113; 25) ‘anonymity-enhancing coins’ means crypto-assets that have built-in features designed to make crypto-asset transfer information anonymous, either systematically or optionally;	
Obliged entities Article 3	
The following entities are to be considered **obliged entities** for the purposes of this Regulation: 3) the following **natural or legal persons** acting in the exercise of their professional activities: (…) b) notaries, lawyers and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning any of the following: (…) (iii) opening or management of bank, savings, securities or **crypto-assets accounts**;	All types and categories of **crypto-asset service providers** (as defined in MiCA) are now **obliged entities.** They will be required to report beneficial ownership information to the bank account register.

Customer due diligence measures Article 19(3)	
3) By way of derogation from paragraph 1, point (b), **crypto-asset service providers** shall: a) **apply customer due diligence measures** when carrying out an occasional transaction that amounts to a **value of at least EUR 1 000**, or the equivalent in national currency, **whether the transaction is carried out in a single operation or through linked transactions**; b) apply at least customer due diligence measures referred to in Article 20(1), point (a), when carrying out an occasional transaction where the **value is below EUR 1 000**, or the equivalent in national currency, **whether the transaction is carried out in a single operation or through linked transactions**.	Under the AML Regulation the threshold for mandatory Customer Due Diligence (CDD) for occasional transactions has been set to **€1,000**. Even for transactions under €1,000, CASPs must still identify the customer (though verification can be simplified).

Specific enhanced due diligence measures for cross-border correspondent relationships for crypto-asset service providers
Article 37

1) (…), with respect to cross-border correspondent relationships involving the **execution of crypto-asset services**, with a respondent entity not established in the Union and providing similar services, including transfers of crypto-assets, crypto-asset service providers shall, **in addition to the customer due diligence measures laid down in Article 20**, when entering into a business relationship, be required to:

(…)

(f) with respect to payable-through crypto-asset accounts, **be satisfied that the respondent entity has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent entity, and that it is able to provide relevant customer due diligence data to the correspondent entity, upon request**.

Where crypto-asset service providers decide to terminate correspondent relationships for reasons relating to AML/CFT policy, they shall document their decision.

(…)

2) Crypto-asset service providers shall take into account the information collected pursuant to paragraph 1 in order to determine, **on a risk sensitive basis**, the appropriate measures to be taken to mitigate the risks associated with the respondent entity.

3) By **10 July 2027**, **AMLA shall issue guidelines to specify the criteria and elements that crypto-asset service providers shall take into account for conducting the assessment referred to in paragraph 1 and the risk mitigating measures referred to in paragraph 2**, including the minimum action to be taken by crypto-asset service providers upon identification that the respondent entity is not registered or licensed.

Certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established with the regular application of customer due diligence measures, there are cases in which particularly rigorous customer identification and verification procedures are required. The Regulation lays down detailed rules on such enhanced due diligence measures, including specific enhanced due diligence measures for cross-border correspondent relationship.

The intensity of the enhanced due diligence measures should be determined by application of the principles of the risk-based approach.

Prohibition of correspondent relationships with shell institutions Article 39(2)	
(…) **crypto-asset service providers** shall ensure that **their accounts are not used by shell institutions to provide crypto-asset services**. To that end, crypto-asset service providers shall have in place internal policies, **procedures and controls to detect any attempt to use their accounts for the provision of unregulated crypto-asset services**.	Given the high risk of money laundering and terrorist financing inherent in shell institutions, credit institutions, financial institutions, and crypto-asset service providers should refrain from entertaining any correspondent relationship with such shell institutions, as well as with counterparts in third countries that allow their accounts to be used by shell institutions.
Measures to mitigate risks in relation to transactions with a self-hosted address Article 40	
1) Crypto-asset service providers shall **identify and assess the risk of money laundering and financing of terrorism** associated with **transfers of crypto-assets** directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Crypto-asset service providers shall **apply mitigating measures commensurate with the risks identified**. (…) 2) By **10 July 2027**, **AMLA shall issue guidelines** to specify the mitigating measures referred to in paragraph 1 (…).	An appropriate risk-based approach requires obliged entities to identify the inherent risks of money laundering and terrorist financing as well as the risks of non-implementation or evasion of targeted financial sanctions. In doing so, obliged entities should take into account the characteristics of their customers, the products, services or transactions offered, including, for crypto-asset service providers, transactions with self-hosted addresses, the countries or geographical areas concerned, and the distribution channels used. In light of the evolving nature of risks, such risk assessment should be regularly updated.

Anonymous accounts and bearer shares and bearer share warrants Article 79	
1) Credit institutions, financial institutions and **crypto-asset service providers** shall be **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 for the **anonymisation of the customer account holder** or the **anonymisation or increased obfuscation of transactions, including through anonymity-enhancing coins**. Owners and beneficiaries of existing anonymous bank or payment accounts, anonymous passbooks, anonymous safe-deposit boxes held by credit institutions or financial institutions, or crypto-asset accounts shall be **subject to customer due diligence measures before those accounts, passbooks, or deposit boxes are used in any way.** (…)	The anonymity of crypto-assets exposes them to risks of misuse for criminal purposes. Anonymous crypto-asset accounts, as well as other anonymising instruments, do not allow the traceability of crypto-asset transfers, and make it difficult to identify linked transactions that might raise suspicion or to apply an adequate level of customer due diligence. In order to ensure effective application of AML/CFT requirements to crypto-assets, it is necessary to prohibit the provision and the custody of anonymous crypto-asset accounts or accounts allowing for the anonymisation or the increased obfuscation of transactions by crypto-asset service providers, including through anonymity-enhancing coins. That prohibition does not apply to providers of hardware and software or providers of self-hosted wallets insofar as they do not possess access to or control over those crypto-asset wallets.

ANTI-MONEY LAUNDERING DIRECTIVE (AMLD)

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
Bank account registers and electronic data retrieval systems Article 16	AMLD6 establishes the Bank Account Register Interconnection System (**BARIS**), a centralised, **EU-wide access point for information** on bank accounts and payment accounts, securities accounts, **crypto-asset accounts** and safe-deposit boxes, to be established by **July 2029.** Centralised automated mechanisms allowing the identification of holders of bank accounts or payment accounts, securities accounts, crypto-asset accounts and accounts and safe-deposit boxes should also be interconnected by that date.
1) Member States shall put in place **centralised automated mechanisms**, such as **central registers or central electronic data retrieval systems**, which allow the **identification, in a timely manner**, of **any natural or legal persons holding or controlling** payment accounts, or bank accounts identified by IBAN, including virtual IBANs, securities accounts, **crypto-asset accounts** and safe-deposit boxes held by a credit institution or financial institution within their territory. (…) 3) The following **information** shall be **accessible and searchable through the centralised automated mechanisms**: (f) for **crypto-asset accounts**: the unique identifier of the account, and the dates of account opening and closing; (…)	

6) The **centralised automated mechanisms** shall be **interconnected** via the **bank account registers interconnection system ('BARIS')**, to be **developed and operated by the Commission**. The Commission shall ensure such interconnection in cooperation with Member States by **10 July 2029**. The Commission may set out, by means of implementing acts, the technical specifications and procedures for the connection of Member States' centralised automated mechanisms to BARIS. (…) 8) Member States shall ensure that **information on holders** of bank accounts or payment accounts, including virtual IBANs, securities accounts, **crypto-asset accounts** and safe-deposit boxes **is made available through their national centralised automated mechanisms and through BARIS** during a period of 5 years after the closure of the account.	**Good practice example** **Italy** In Italy, financial and credit institutions are already required to report information on crypto asset accounts to the bank account register. Starting in December 2024, crypto-asset service providers were also legally recognised as financial institutions in Italy. However, the practical implementation of this requirement is still under discussion.
Access to information Article 21	
1) Member States shall ensure that **FIUs**, regardless of their organisational status, **have access to the information that they require to fulfil their tasks**, including financial, administrative and law enforcement information. Member States shall ensure that FIUs have at least: (a) **immediate and direct access** to the following financial information: (…) (ii) **information from obliged entities**, including information on transfers of funds as defined in Article 3, point (9), of Regulation (EU) 2023/1113 and **transfers of crypto-assets** as defined in Article 3, point (10), of that Regulation;	Through the interconnection of Member States' centralised automated mechanisms, **national FIUs would be able to obtain swiftly cross-border information on the identity of holders of bank accounts and payment accounts, securities accounts, crypto-asset accounts and safe deposit boxes in other Member States**, which would reinforce their ability to effectively carry out financial analysis and cooperate with their counterparts from other Member States.

Suspension or withholding of consent Article 24(2)	
Where there is a **suspicion** that a bank account or payment account, **a crypto-asset account** or a business relationship is **related to money laundering or terrorist financing**, Member States shall ensure that the **FIU is empowered to take urgent action**, directly or indirectly, **to suspend the use of that account or to suspend the business relationship in order to preserve the funds, to perform its analyses, to assess whether the suspicion is confirmed and if so, to disseminate the results of the analyses** to the relevant competent authorities to allow for the adoption of appropriate measures. (…) Member States shall ensure that FIUs exercise their function subject to **appropriate national safeguards**, such as the possibility for the person whose bank account or payment account, crypto-asset account or business relationship is suspended to challenge that suspension before a court.	//
Instructions to monitor transactions or activities Article 25	
Member States shall ensure that **FIUs are empowered to instruct obliged entities to monitor**, for a period to be specified by the FIU, **the transactions or activities** that are being carried out through one or more bank accounts or payment accounts or **crypto-asset accounts** or other business relationships managed by the obliged entity **for persons who present a significant risk of money laundering, its predicate offences or terrorist financing**.	//

Supervision of forms of infrastructure of certain intermediaries operating under the freedom to provide services Article 38(1)	
Where the activities of the **following obliged entities** are carried out in their territory under the **freedom to provide services** through agents or distributors, or through other types of infrastructure (…), Member States shall ensure that such activities are **subject to supervision by their national supervisors**: (…) (c) crypto-asset service providers.	//
Central contact points Article 41(1)	
For the purposes of Article 37(1) and Article 38(1), Member States may require electronic money issuers, payment service providers and **crypto-asset service providers operating establishments in their territory other than a subsidiary or a branch**, **or** operating in their territory **through agents or distributors, or through other types of infrastructure**, under the freedom to provide services, **to appoint a central contact point in their territory**. That central contact point shall ensure, on behalf of the obliged entity, **compliance with AML/CFT rules** and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.	In light of anti-money laundering vulnerabilities related to electronic money issuers, payment service providers and crypto-assets service providers, it should be possible for Member States to require that those providers established on their territory in forms other than a branch or through other types of infrastructure and the head office of which is located in another Member State **appoint a central contact point**. Such a central contact point, acting on behalf of the appointing institution, should ensure the establishments' compliance with AML/CFT rules.

ANTI-MONEY LAUNDERING AUTHORITY REGULATION (AMLA)

RELEVANT LEGISLATION

Regulation (EU) 2024/1620 of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (known as the AMLA Regulation)

PROVISIONS	EXPLAINER
Tasks Article 5(2)	
The Authority shall perform the following tasks with respect to **selected obliged entities**: (a) **ensure compliance** of the selected obliged entities with the requirements applicable to them pursuant to Regulation (EU) 2024/1624 and Regulation (EU) 2023/1113, (…); (…) (b) carry out **supervisory reviews and assessments** at the level of individual entities and at group-wide level in order to determine whether the internal policies, procedures and controls put in place by the selected obliged entities are adequate to comply with the requirements applicable to them, and on the basis of those supervisory reviews and assessments impose specific requirements, **apply administrative measures and impose pecuniary sanctions and periodic penalty payments** pursuant to Articles 21, 22 and 23; (c) **participate in group-wide supervision**, in particular in AML/CFT supervisory colleges, including where a selected obliged entity is part of a group that has headquarters, subsidiaries or branches outside the Union; (d) develop and keep up to date a system to **assess the risks and vulnerabilities of the selected obliged entities**, (…)	As stated above, the Single Rulebook **AML Regulation (EU) 2024/1624**, which will apply directly across the Union and, expressly brings **CASPs into the list of "obliged entities"**. Application is set for **10 July 2027** (with certain sectoral deferrals). The AMLA is the new **Anti-Money Laundering and Countering the financing of Terrorisms Authority**, based in Frankfort. It was established in 26 June 2024 and will be fully operational in January 2028. The decentralised agency will coordinate national authorities to ensure the correct and consistent application of EU AML rules. In 2027, AMLA will select 40 obliged entities which will be subject to direct supervision. AMLA's 2025 Workplan names **crypto-related** crime as an "**immediate priority**" for the year citing inconsistent supervision of CASPs (now required to get a MiCA licence to operate in the EU) across member states as a key vulnerability. To address this, the agency will work closely with national regulators and begin coordinating with financial intelligence units to track cross-border crypto risks.

Assessment for credit institutions and financial institutions for the purposes of selection for direct supervision Article 12	
1) For the purposes of carrying out the tasks listed in **Article 5(2)**, the Authority, in collaboration with financial supervisors, **shall carry out a periodic assessment of credit institutions and financial institutions**, and groups of credit institutions and financial institutions, where they operate, whether through establishments or under the freedom to provide services, **in at least six Member States**, including the home Member State, regardless of whether the activities are carried out through infrastructure on the territory concerned or remotely. 2) The supervisory authorities, and the obliged entities subject to periodic assessment, **shall supply the Authority with any information necessary to carry out the periodic assessment** referred to in paragraph 1. 3) The **inherent and residual risk profiles** of an obliged entity assessed pursuant to paragraph 1 shall be classified by the Authority as **low, medium, substantial or high**, based on the benchmarks and following the methodology set out in the regulatory technical standards referred to in paragraph 7. (…). The **methodology for classifying inherent and residual risk profiles** shall be established separately for at least the following categories of obliged entities: (…)	The upcoming **Commission's delegated regulation** will lay out regulatory technical standards specifying the methodology for assessing obliged entities for the purposes of the **selection for direct supervision.** According to the draft, if the activities of the obliged entity under the freedom to provide services **in at least five Member States** other than where it is established shall be considered **material** where: a) the number of its customers that are resident in that Member State is above 20.000 b) the total value in Euro of incoming and outgaining transaction generated by those costumers is above EUR 50 million.

(j) crypto-asset service providers; 5) For each category of obliged entities referred to in paragraph 4, the benchmarks for the assessment of inherent risk in the assessment methodology shall be based on the risk factor categories related to customers, products, services, transactions, delivery channels and geographical areas. The benchmarks shall be established for at least the following indicators of inherent risk in any Member State in which the obliged entities operate: (a) (…) (b) (…) (c) with respect to geographical areas: (i) the **annual volume** of correspondent banking services and **correspondent crypto-asset services**, provided by **Union** financial sector entities in third countries identified pursuant to Chapter III, Section 2, of Regulation (EU) 2024/1624; (ii) the **number and share of correspondent** banking clients and crypto-asset clients in **third countries** identified pursuant to Chapter III, Section 2, of Regulation (EU) 2024/1624.	

FINANCIAL ACTION TASK FORCE RECOMMENDATIONS (FATF)

LEGAL TEXT

Recommendations of the Financial Action Task Force (FATF)

PROVISIONS	EXPLAINER
Terms and definitions	
Virtual asset: is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are covered elsewhere in the FATF Recommendations. **Virtual asset service providers**: any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: • Exchange between virtual assets and fiat currencies • Exchange between one or more forms of virtual assets	Countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs).

New technologies Recommendation 15	
Countries and financial institutions should identify and assess **the money laundering or terrorist financing risks** that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. To manage and mitigate **the risks emerging from virtual assets**, countries should ensure that **virtual asset service providers are regulated for AML/CFT purposes**, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.	According to recommendation 15, countries must ensure VASPs are regulated, licensed or registered. VASPs must comply with AML/CFT obligations, including monitoring, supervision and enforcement in line with FATF standards.
Payment transparency Recommendation 16	
Countries should ensure that financial institutions include required and **accurate originator information,** and required **beneficiary information**, on payments or value transfers and related messages. This information should be structured to the extent possible and should remain with such payment or value transfer or related message throughout the payment chain. Countries should ensure that **financial institutions monitor payments or value transfers** for the purpose of detecting those which lack required originator and/or beneficiary information and take appropriate measures. (…)	Recommendation 16 requires countries to ensure that payments and value transfers are transparent and traceable to prevent AML/CFT. • Payments must include accurate originator (sender) and beneficiary (receiver) information. • The information should be structured and must travel with the payment through the entire payment chain.

DORA REGULATION

RELEVANT LEGISLATION

Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector
(known as the DORA Regulation)

PROVISIONS	EXPLAINER
Scope Article 2	The Digital Operational Resilience Act, known as DORA, addresses a critical gap in EU financial regulation. **Prior to DORA, financial institutions primarily managed operational risks by allocating capital to cover potential losses**. This approach failed to encompass all aspects of operational resilience, particularly in relation to Information and Communication Technology (ICT). With the introduction of DORA, financial institutions are now required to follow stringent guidelines for safeguarding against ICT-related incidents. These include measures for protection, detection, containment, recovery, and repair. **DORA explicitly targets ICT risks**, introducing clear rules for ICT risk management, incident reporting, operational resilience testing, and oversight of ICT third-party risks. See MiCA Regulation for the definitions of '**crypto-asset service provider'** and **'issuer of asset-referenced tokens'**
1)(a) Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities: (…) (f) **crypto-asset service providers** as authorised under a Regulation on markets in crypto-assets, and **issuers of asset-referenced tokens**;	

Competent authorities Article 46	
Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers, compliance with this Regulation shall be ensured by the following competent authorities in accordance with the powers granted by the respective legal acts: (...) (d) for **crypto-asset service providers** as authorised under the Regulation on markets in crypto-assets and issuers of asset-referenced tokens, the competent authority designated in accordance with the relevant provision of that Regulation (…)	DORA includes crypto-asset service providers among financial entities that fall under its resilience and operational risks requirements. It applies to crypto-asset providers that are authorised under the MiCA Regulation, and to issuers of asset-referenced tokens.

DAC8 DIRECTIVE

RELEVANT LEGISLATION

Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (known as the DAC8 Directive)

PROVISIONS	EXPLAINER
Scope and conditions of mandatory automatic exchange of information reported by Reporting Crypto Asset Service Providers Article 8ad	
1) Each Member State shall take the necessary measures to **require Reporting Crypto-Asset Service Providers to fulfil the reporting requirements and carry out the due diligence procedures** laid down in Sections II and III of Annex VI, respectively. Each Member State shall also ensure the effective implementation of, and compliance with, such measures in accordance with Section V of Annex VI. 2) (…) the competent authority of a Member State where the reporting referred to in paragraph 1 of this Article takes place shall, by means of **automatic exchange**, and within the time limit laid down in paragraph 6 of this Article, communicate the information specified in paragraph 3 of this Article to the competent authorities of the Member States concerned in accordance with the practical arrangements adopted pursuant to Article 21. 3) The competent authority of a Member State shall communicate the following information regarding each Reportable Person:	Objective: the directive does not deal with the charging and payment of taxes itself, but rather allows for the collection and (increasingly automatic) **exchange between Member States of tax-related information about individuals and companies**. This allows national tax administrations to track and cross-check income streams, stop cases of tax fraud and evasion and impose taxes where required according to national legislation. Article 8ad requires that info collected by a CASP in one Member State is automatically sent to the tax office of the user's home country. It prevents citizens from hiding capital gains in offshore or cross-border crypto accounts.

(…) (c) for **each type of Reportable Crypto-Asset** with respect to which the Reporting Crypto-Asset Service Provider has effectuated Reportable Transactions during the relevant calendar year or other appropriate reporting period, where relevant: (…) (ii) the aggregate gross amount paid, the aggregate number of units and the number of Reportable Transactions in respect of acquisitions against Fiat Currency;	
Penalties Article 25a	The Directive introduces a common minimum level of penalties for “serious” non-compliance (like failure to report).
Member States shall lay down the rules on **penalties applicable to infringements of national provisions adopted pursuant to this Directive** and concerning Articles 8aa to 8ad, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.	
Annex VI	//
This Annex lays down the reporting requirements, due diligence procedures and other rules to be applied by the Reporting Crypto-Asset Service Providers in order to enable Member States to communicate, by automatic exchange, the information referred to in Article 8ad.	

Due Diligence Procedure **Annex VI, Section III**	
A Crypto-Asset User is treated as a Reportable User beginning as of the date when it is identified as such pursuant to the due diligence procedures described in this Section. (…) A1. When establishing the relationship with the Individual Crypto-Asset User, (…), **the Reporting Crypto-Asset Service Provider shall obtain a self-certification that allows the Reporting Crypto-Asset Service Provider to determine the Individual Crypto-Asset User's residence(s) for tax purposes** and confirm the reasonableness of such self-certification **based on the information obtained by the Reporting Crypto-Asset Service Provider, including any documentation collected pursuant to Customer Due Diligence Procedures**. (…) C. Requirements for validity of self-certifications (…) (d) with respect to each Reportable Person, the TIN with respect to each Member State;	CASPs must not only identify users (KYC) but specifically collect their Tax Identification Number (TIN) and place of birth. This allows tax authorities to perfectly match a crypto account to a specific tax return.

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