# Markets in Crypto-Assets Regulation (MiCA)

**A comprehensive guide for Crypto-Asset Service Providers (CASPs)**

August 2025

kpmg.com.cy

# Table of contents

# Introduction: navigating the new crypto landscape

### 1.1 Understanding the Markets in Crypto-Assets Regulation (MiCA)

The Markets in Crypto-Assets Regulation (EU) 2023/1114, fully applicable since 30 December 2024, represents the EU's first comprehensive regulatory framework for crypto-assets and related services. MiCA harmonises rules across all EU Member States, replacing fragmented national regimes and providing legal certainty for businesses and consumers alike. Its primary objectives are to protect consumers, enhance market integrity, and foster innovation in the rapidly evolving crypto sector, positioning the EU as a leader in responsible crypto-asset development.

### 1.2 MiCA scope: key categories of crypto-assets

MiCA broadly defines crypto-assets as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology".

The regulation recognises three main categories of crypto-assets based on their characteristics and associated risk profiles, each subject to different requirements:

| Category | Definition and uses | Examples | Key regulatory focus |
|---|---|---|---|
| **E-money tokens (EMTs)** | **Tokens aiming to maintain a stable value by referencing a single official currency (e.g., euro, USD), aligning with the E-Money Directive (EMD2). Primarily used for payments and redeemable at face value.** | **USD Coin (USDC), Tether (USDT).** | **Maintaining stability and robust redemption mechanisms.** |
| **Asset-Referenced Tokens (ARTs)** | **Tokens seeking to stabilise their value by referencing multiple assets (currencies, commodities, other crypto-assets). Designed for broader stability and value preservation.** | **Paxos Standard (PAX), DAI (if multi-asset backed).** | **Ensuring adequate backing assets and managing potential systemic risks.** |
| **Other crypto-assets** | **All other crypto-assets not classified as EMTs or ARTs. Including utility tokens that grant access to specific goods, services, or platforms, as well as widely known cryptocurrencies.** | **Ether (ETH), Basic Attention Token (BAT), Chiliz (CHZ).** | **Establishing conduct of business rules and ensuring market transparency.** |

From the categories in the table above, MiCA clearly covers a wide range of crypto-assets — not only widely known cryptocurrencies like Bitcoin and Ethereum, but also stablecoins (e-money tokens and asset-referenced tokens), and utility tokens that provide digital access to applications, services, or platforms.

The European Banking Authority (EBA) classifies ARTs and EMTs as significant if they meet at least three criteria outlined in MiCA, such as:

- Large user base
- High market capitalisation
- Systemic importance to payment systems.

Issuers of significant tokens face stricter requirements, such as enhanced capital reserves, stress-testing protocols, and direct oversight by the EBA, reflecting the higher potential impact of these assets.

### 1.3 Excluded crypto-assets under MiCA

Crypto-assets not covered by MiCA

MiCA excludes crypto-assets already subject to existing EU financial legislation, preventing regulatory overlap. These include:

- Traditional financial instruments: Including those tokenised under MiFID II (e.g., tokenised stocks or bonds).
- Deposits: As defined by the Deposit Guarantee Schemes Directive (DGSD).
- Investment funds: Such as UCITS or AIFs (unless they qualify as EMTs).
- Securitisation positions: Insurance and Pension Products.
- Central Bank Digital Currencies (CBDCs) and crypto assets issued by central banks in their monetary policy capacity.
- Non-Fungible Tokens (NFTs) are generally excluded, with caveats:
    - NFTs issued in large series or collections may be deemed fungible and fall under MiCA.
    - Fractionalised NFTs (where ownership of a single NFT is divided) do not benefit from the exclusion.

### 1.4 Entities in scope under MiCA

MiCA applies to any legal person or other entity that:

- Issues, offers, or seeks to admit crypto-assets to trading within the EU.
- Professionally provides crypto-asset services as a business activity within the EU such entities are known as Crypto-Asset Service Providers (CASPs).

This guide specifically focuses on the requirements and procedures for obtaining and maintaining authorisation as a CASP under MiCA, outlining the ongoing obligations essential for compliance.

# Crypto-Asset Service Providers (CASPs) under MICA: your gateway to the EU market

### 2.1 Defining the CAPS

Under Article 3(1)(15) of MiCA, a CASP is any legal entity or undertaking that professionally provides one or more regulated crypto-asset services to clients located within the EU. This broad definition encompasses a range of activities crucial to the crypto ecosystem.

### 2.2 Authorisation routes

Entities wishing to provide crypto-asset services within the European Union must fall into one of two categories:

**Authorised CASPs**

Entities must generally obtain specific authorisation as a CASP from their home Member State's competent authority (Article 59 of MiCA). This applies to legal persons and certain eligible non-legal entities[1]

**Exempt financial entities:**

Certain established financial entities benefit from a streamlined notification procedure, allowing them to provide crypto-asset services under their existing licenses. These include:

- Credit institutions
- Central securities depositaries
- Investment firms
- Market operators
- Electronic money institutions
- UCITS management company or alternative investment fund managers.

This reflects the EU's recognition of the existing regulatory oversight and experience of these entities.

Please see paragraph 6.3 in this publication for more information.

### 2.3 Regulated crypto-asset services under MiCA

Article 3(1)(9) of MiCA defines the following as crypto-asset services requiring authorisation, each with specific obligations:

**Class 1**

- Execution of orders for crypto-assets on behalf of clients;
- Placing of crypto-assets;
- Providing transfer services for crypto-assets on behalf of clients;
- Reception and transmission of orders for crypto-assets on behalf of clients;
- Providing advice on crypto-assets;
- Providing portfolio management on crypto-assets.

**Class 2**

- Providing custody and administration of crypto-assets on behalf of clients;
- Exchange of crypto-assets for funds (fiat)
- Exchange of crypto assets for other crypto-assets.

**Class 3**

- Operation of a trading platform for crypto-assets.

[1] Non-legal persons may apply for authorisation only if their legal structure provides third-party protection equivalent to that of legal persons and if they are subject to appropriate prudential supervision for their specific legal form.

# CASP authorisation process

### 3.1 Application documentation (Article 62 of MiCA): building your authorisation file

Under MiCA, any entity intending to provide crypto-asset services within the European Union must obtain prior authorisation from the competent authority of its home Member State. In Cyprus, this authority is the Cyprus Securities and Exchange Commission (CySEC), which is responsible for the authorisation and on-going supervision of CASPs.

To obtain authorisation in Cyprus, a company must be legally established in the country and demonstrate effective management. CySEC expects that the majority of board members be based in Cyprus and actively involved in decision-making, which also supports the entity's tax residency status. Additionally, at least half of the board should consist of independent non-executive directors to ensure robust governance and oversight.

The authorisation process requires applicants to meet strong organisational and conduct standards similar to those for traditional financial services. They must submit a detailed application to the authority, showing they are ready to operate under MiCA in terms of their operations, technology, governance, and compliance.

Key required documents typically include:

| | |
|---|---|
| **General information** | • Legal form and registered address.<br>• Articles of Association/constitutional documents.<br>• Legal Entity Identifier (LEI).<br>• Website domain and social media accounts. |
| **Programme of operations** | • Services and activities: Overview of requested services and the types of crypto-assets involved.<br>• Group strategy and structure: Group interactions, ownership structure, and qualifying shareholders (as applicable).<br>• Geographic scope and clients: Target markets inside and outside the EU, client profiles, access methods, and applicable non-EU regulations.<br>• Marketing and promotion: Communication channels, marketing strategies, target audiences, and languages used.<br>• Resources and location: Summary of human, financial, and ICT resources, and location of key operational functions.<br>• Outsourcing entities: Details of outsourced service providers, their locations, and functions performed.<br>• Financials: 3-year forecasts with stress testing, group-level breakdowns, capital adequacy, and intra-group funding (as applicable). |
| **Proof of prudential safeguards** | • Proof of initial capital, safeguards, and insurance.<br>• Description of capital monitoring and compliance processes. |
| **Governance arrangements description** | • Robust governance arrangements with effective oversight mechanisms.<br>• Clear organisational structure with well-defined responsibilities and lines of accountability. |

# CASP authorisation process

| | |
|---|---|
| **Members of the management body information:** | • Each board member must submit information including proof of identity, residence history, positions held and corresponding start dates, a CV highlighting experience in finance, technology, and crypto, a criminal record certificate, and any relevant disclosures. They must also provide details on time commitment and any external mandates. |
| **Shareholder information on qualifying holdings** | • Identification of individuals or entities with qualifying holdings (i.e. at least 10% direct or indirect ownership).<br>• Evidence of their good repute and financial soundness. |
| **Business continuity plan and operational resilience** | • Develop thorough business continuity plans to maintain services during disruptions, including data recovery and crisis response.<br>• Regularly test recovery and backup systems.<br>• Identify key business functions and set practical recovery time goals. |
| **Internal operation manual** | Applicants must maintain a robust internal rulebook that ensures operational integrity, covering:<br>• Governance & controls: Clear reporting lines and internal control mechanisms.<br>• Risk management: Policies to identify, assess, and mitigate operational, financial, and compliance risks.<br>• Complaints handling: Procedures for receiving, investigating, and resolving client complaints.<br>• Conflict of interest: Defined protocols for managing and escalating conflicts.<br>• Client asset safeguards: Measures for asset segregation, custody, and reconciliation.<br>• Outsourcing & contingency: Oversight of critical service providers, with fallback arrangements in place.<br>• Record-keeping: Systems to ensure secure, auditable data management.<br>• Service-specific policies: Tailored procedures for each crypto-asset service, including delivery, monitoring, compliance, and client handling. |
| **AML/CFT and risk management policies:** | • AML manual and sanctions policy, systematic Integrity Risk Assessment (SIRA), comprehensive risk frameworks covering market, operational, and liquidity risks, and AML risk mapping by client type, service, and region. |

# CASP authorisation process

| | |
|---|---|
| **Technical documentation of the ICT systems and security arrangements:** | • Security policies, system setup, and GDPR-compliant ICT governance.<br>• Assessment of critical ICT functions and service provider contracts.<br>• Incident response plans with clear breach reporting.<br>• Regular security tests and audits to identify and remediate potential risks.<br>• IT and cybersecurity measures to protect client data, including access controls and encryption.<br>• Compliance with DORA requirements.<br>• Plain-language summary for the regulator. |
| **Depending on services offered** | • Trading platform rules and market abuse preventions systems.<br>• Confirmation of competence for crypto advisors and portfolio managers. |

*The CySEC may request further information or clarifications during the assessment process.*

### 3.2 Timeframes for examining the application (Article 63 of MiCA)

| Step | Description | Timeline |
|---|---|---|
| **Acknowledgement of receipt** | Authorities confirm they have received the application. | Within 5 working days |
| **Application completeness review** | Authorities review if the application is complete. | Within 25 working days |
| **Final decision** | Authorities issue approval or refusal of the application. | Within 40 working days from receipt of a complete application* |

**Note: Timelines may pause if additional information is requested*

- EU passporting: Once authorised, CASPs gain EU-wide operating rights under a single license (Article 67 of MiCA).
- Public register: ESMA will list all authorised CASPs in an official EU register (Article 71 of MiCA).

# CASP authorisation process

### 3.3 CYSEC fees

| Fee Type | Amount (€) |
|---|---|
| **CASP application fees** | A flat fee of €8,000 non-refundable payable upon submission of the application for each proposed service.<br><br>Note: Successful applicants are not required to pay an additional annual fee for the first year of registration. |
| **CASP annual supervision fees** | The fee structure has a fixed and a variable component.<br><br>The fixed component is based on the services provided:<br>• Custody and administration of crypto-assets - €10,000 per year.<br>• Operation of a trading platform - €20,000 per year.<br>• Exchange of crypto-assets for funds - €5,000 per year<br>• Exchange of crypto-assets for other crypto-assets - €5,000 per year<br>• Execution of orders on behalf of clients - €5,000 per year.<br>• Placing of crypto-assets - €5,000 per year.<br>• Reception and transmission of orders - €5,000 per year.<br>• Providing advice on crypto-assets - €8,000 per year.<br>• Providing portfolio management - €8,000 per year.<br>• Providing transfer services - €5,000 per year.<br>Notes:<br>The fixed component is payable annually from the second year of registration onwards.<br>The annual supervision fee is payable within four months after the end of the CASP's financial year. |
| | The variable component is based on the annual financial turnover from crypto-asset services, applicable if turnover exceeds €500,000.<br>Note: The calculation of the variable component is based on the audited financial statement of the previous year.<br>The variable fee scale is approximately:<br>• 1% for turnover €500,001– €1,000,000<br>• 0.4% for turnover €1,000,001– €5,000,000<br>• 0.3% for turnover €5,000,001– €10,000,000<br>• 0.1% for turnover above €10,000,000<br>The total annual supervisory fee is capped at €500,000 |
| **Fees for notifications & modifications** | Notification of Board of Directors changes: €2,000 fee applies for each change. |
| **Other potential fees** | Annual ICT oversight fees that vary based on the entity's classification under the Digital Operational Resilience Act (DORA). While DORA is a separate regulation, it also applies to CASPs as financial entities. |

# CASP authorisation process

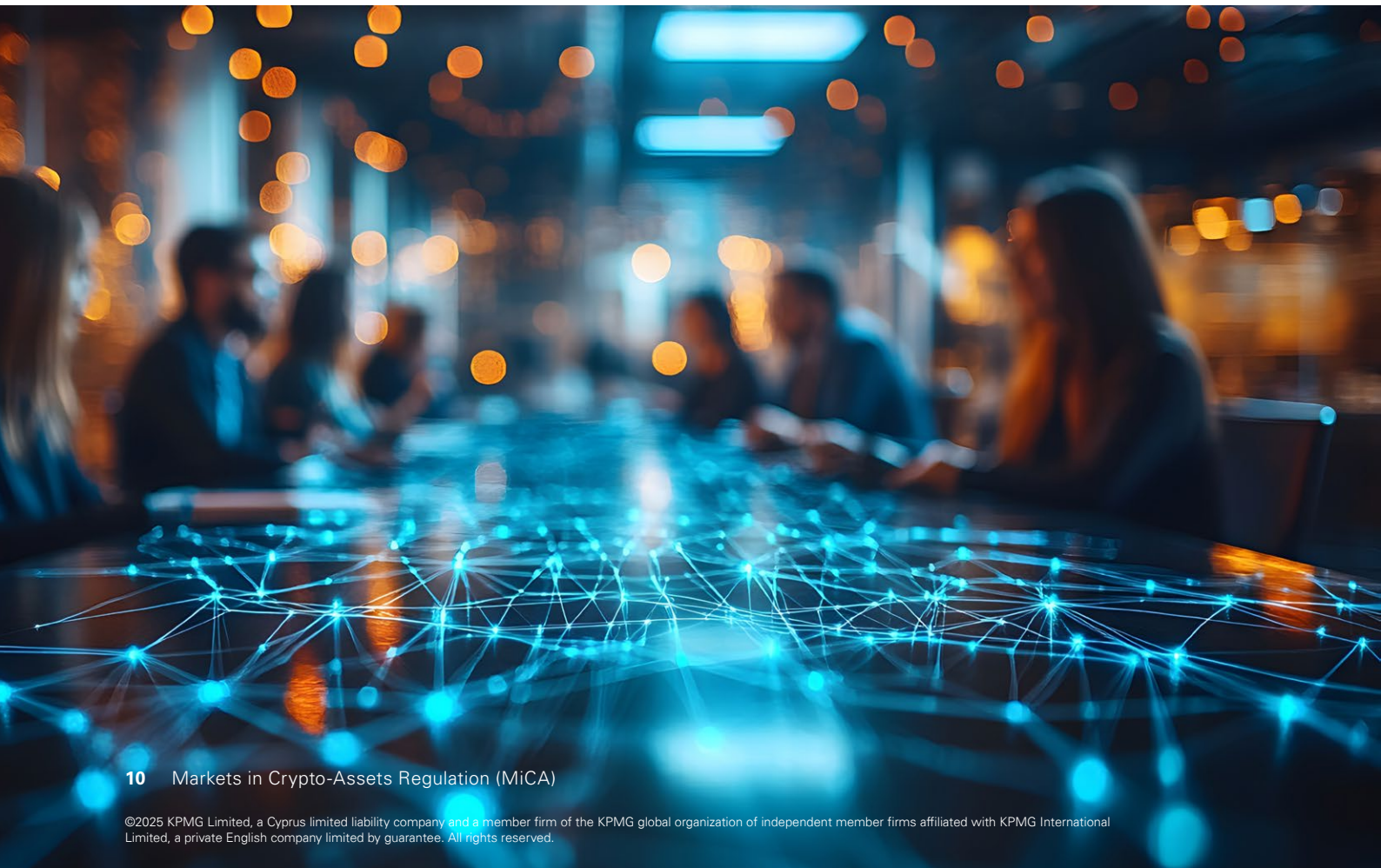
### 3.4 Prudential capital and overhead requirements for CASPs

CASPs must meet specific initial and ongoing capital requirements, based on the type of services offered:

| Service class | Description of services | Minimum capital |
|---|---|---|
| **Class 1** | Execution of orders, order reception/ transmission, investment advice, portfolio management, placing and transfer services | €50,000 |
| **Class 2** | Custody, crypto-to-fiat exchanges, and crypto-to-crypto exchanges | €125,000 |
| **Class 3** | Operation of trading platforms | €150,000 |

- CASPs will need to maintain at all times at least this minimum capital requirement, or a quarter of the fixed overheads of the firm in the preceding year (to be reviewed annually), whichever is greater.

- Capital requirements can be met through own funds (Common Equity Tier 1 items, as defined under the Capital Requirements Regulation), and/or a qualifying insurance policy. Such insurance must cover operational risks including system failures, misstatements, documentation loss, conflicts of interest, safeguarding failures, and liability for client asset loss.



# Ongoing obligations for authorised CASPs: maintaining compliance

Once authorised, CASPs must continuously comply with a comprehensive set of obligations aimed at safeguarding clients and maintaining market integrity. These requirements cover multiple areas of their operations:

**Additional requirements for specific services:**

Specific obligations for a CASP vary depending on the services they intend to provide:

| Area | Key requirements and responsibilities | Specific actions |
|---|---|---|
| **Client protection** | | |
| Best interest of clients (Art. 66 MiCA) | Act honestly, fairly, and professionally; prioritise clients' interests | Provide transparent, clear information including risks, fees, environmental impact; share white papers (as applicable) |
| Complaints handling (Art. 71 MiCA) | Clear, accessible procedures | Prompt investigations, defined timelines, full records |
| Client asset safeguarding (Art. 70 MiCA) | Protect ownership rights, segregate assets | Use segregated accounts, deposit with credit institutions/central banks by the next business day, regular reconciliation, insolvency protections |
| Record Keeping | Detailed, secure, retained | All service activities, data retention, secure systems |
| Client communication & disclosure | Transparency | Disclose environmental impact, conflicts of interest, risks, costs |
| **Operational requirements** | | |
| Prudential safeguards (Art. 67 MiCA) | Maintain adequate capital | Minimum capital based on service type and ratios; ongoing review<br>Cover by own funds/appropriate insurance coverage or combination of both |
| Governance (Art. 68 MiCA) | Robust management & compliance | Qualified members, regular reviews, business continuity, secure records |
| Risk management | Policies & procedures | Cover operational, legal, financial, reputational, ICT risks; escalation protocols |
| Conflicts of interest (Art. 72 MiCA) | Proactively manage | Policies to identify, prevent, disclose; annual review |
| Outsourcing (Art. 73 MiCA) | Maintain control & oversight | Due diligence, clear contracts, contingency plans, supervise providers, protect data |
| Wind-down planning (Art. 74 MiCA) | Ensure an orderly cessation of activities if necessary | Develop detailed plans for winding down operations, recovering assets, and minimising harm to clients and markets. |

## Ongoing obligations for authorised CASPs: maintaining compliance

| Area | Key requirements and responsibilities | Specific actions and explanations |
|---|---|---|
| **Service-specific requirements** | | |
| Custody & administration | Client agreements, strong security measures (cold storage/multiple signature), segregation | Quarterly statements, liability for losses, use of authorised providers |
| Trading platforms | Transparent rules, system resilience | Anti-abuse, no proprietary trading, 24-hour settlement, data retention (5 yrs) |
| Exchange services | Non-discriminatory, transparent | Published prices, execution policies, liquidity safeguards, AML/CFT |
| Order Execution | Best execution practices (price, speed, cost) | Clear policies, client consent for off-platform routing |
| Crypto-asset Placement | Due diligence & disclosures | Asset issuer checks, clear terms, conflict controls |
| Order reception/transmission | Accurate, timely, secure | No inducements for routing, data misuse prevention |
| Advice & portfolio management | Suitability & transparency | Client profiling, independence, regular reviews (min. every 2 years); provision of reports |
| Transfer services | Clear client agreements | Secure monitoring, AML/CFT integration |

# Significant CASPs: enhanced oversight

Certain CASPs that reach a significant scale within the EU are subject to enhanced oversight:

**Definition of a Significant CASP**

- A CASP is considered significant if it has at least 15 million active users within the EU.
- Calculation Method: The threshold is determined based on the average number of daily active users over the entire previous calendar year.

**Notification Requirements**

- Timely Notification: Providers must notify their competent authorities within two months after surpassing the threshold.
- Authority Confirmation: Once the competent authority confirms that the threshold is met, they will notify ESMA accordingly.

# Provision of crypto-asset services by regulated financial entities

### 6.1 Scope and equivalence principle

The scope of permitted crypto-asset services under this notification regime is intentionally limited. Regulated financial entities may only offer crypto-asset services that are equivalent to the financial services for which they are already authorized under existing financial regulations. This "equivalence principle" ensures these firms do not operate beyond their established regulatory perimeter without undergoing a more comprehensive assessment.

### 6.2 Notification requirements

Entities aiming to provide crypto-asset services under this regime must submit a detailed notification to the competent authority, including:

- A comprehensive operations programme outlining intended crypto-asset activities
- Evidence of robust internal controls for AML and CTF compliance
- Details on ICT systems and security arrangements to safeguard operations and assets
- Clear procedures for segregation of client crypto-assets to prevent unauthorised use
- Service-specific information relevant to the crypto-asset activities proposed

### 6.3 Simplified access by entity type

The following table summarises the permissible crypto-asset services accessible to different types of regulated financial entities under this notification regime:

| Regulated entity type | Permissible crypto-asset services (upon notification) |
|---|---|
| **Credit Institutions** | All crypto-asset services, including the issuance of asset-referenced tokens (ARTs). |
| **Central Securities Depositories (CSDs)** | Custody and administration of crypto-assets. |
| **Investment Firms** | Crypto-asset services equivalent to their authorised investment services under MiFID II (e.g., reception and transmission of orders, execution of orders, dealing on own account, portfolio management, investment advice). |
| **Electronic Money Institutions (EMIs)** | Custody and administration of e-money tokens they issue, and transfer of e-money tokens they issue. |
| **UCITS management Companies (ManCos)** | Portfolio management of crypto-assets and, subject to additional permissions, investment advice and reception and transmission of orders relating to crypto-assets. |
| **Alternative Investment Fund Managers (AIFMs)** | Portfolio management of crypto-assets and, subject to additional permissions, investment advice and reception and transmission of orders relating to crypto-assets. |
| **Market operators** | Operation of trading platforms for crypto-assets. |

#### "Top-Up" licensing mechanism

This regime offers a "top-up" licensing framework, allowing established entities to expand into crypto-asset services using their existing regulatory compliance frameworks. This option is contingent upon satisfying notification requirements and limiting their crypto-asset activities to those aligned with their current authorisations.

# Additional considerations

### 7.1 MiCA and AML

The revised Transfer of Funds Regulation (EU) 2023/1113 (TFR) entered into force on the same day as MiCA. It requires CASPs to collect and make accessible certain information about the originator and the beneficiary of crypto-asset transfers operated by them to ensure traceability (known as the 'travel rule').

Unlike transfers of funds, the travel rule applies to all crypto-asset transfers involving a CASP regardless of the amount transferred. There are limited exclusions to this rule.

### 7.2 Cross-border service provision

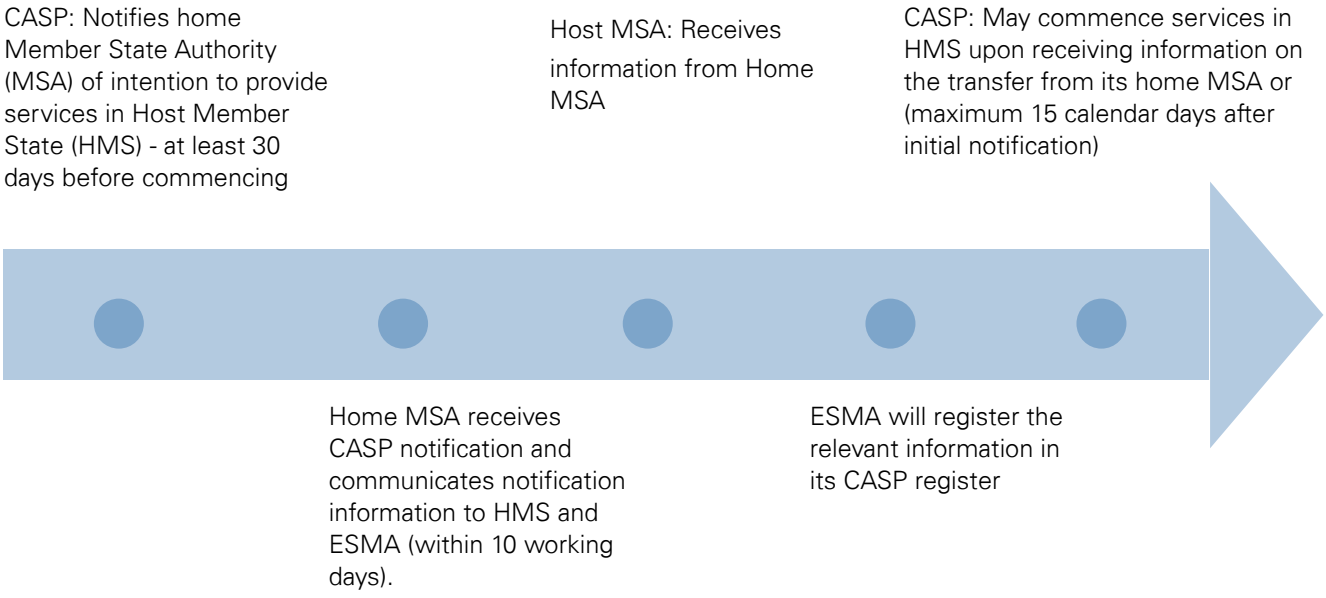
Authorised CASPs benefit from the EU Passport, allowing them to operate across the European Economic Area (EEA) without needing separate authorisation in each country.

Key features:

- Single authorisation: Enables service provision throughout the EEA, with or without physical presence.
- Streamlined process: CASPs notify their home authorities of their targeted EEA countries and the specific services to be offered

This notification activates the passporting process, unlocking access to multiple EU markets under a unified regulatory framework.

The process of exercising this European Passport is as follows:

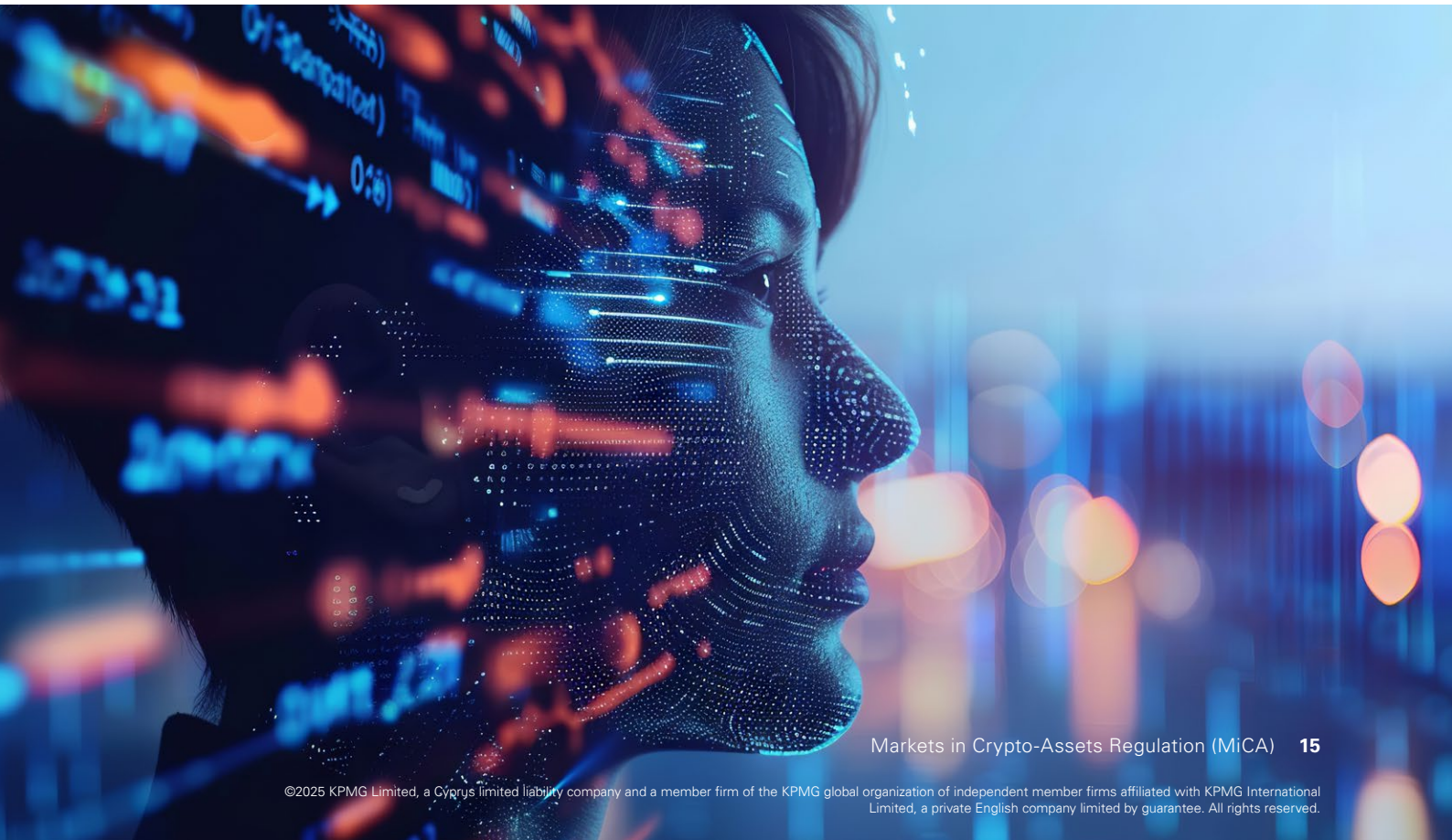


# How we can support you

Our dedicated regulatory advisory team specialises in delivering tailored solutions to help clients navigate and comply with the latest EU regulatory landscape. We assist you in understanding the new requirements introduced by MiCA and integrating them seamlessly into your broader digital asset strategies.

**Our range of services includes:**

- Strategic assessment: Identifying opportunities and benefits arising from digital assets, cryptocurrencies, and underlying technologies.
- Implementation support: Conducting comprehensive regulatory gap analyses, preparing authorisation applications, and developing the necessary operational capabilities.
- Compliance framework development: Designing bespoke AML/CFT, governance, and risk management frameworks to meet regulatory standards.
- Technical readiness: Evaluating and strengthening your IT and cybersecurity infrastructure to ensure compliance with MiCA requirements.
- Tax & audit advisory: Supporting fiscal reporting obligations and ensuring alignment with financial audit standards.
- Regulatory engagement: Acting as your liaison with authorities for licensing, license amendments, and other regulatory interactions.
- Authorisation preparation: Developing and reviewing all application documentation to optimise approval prospects.
- Ongoing compliance support: Offering continued advisory services to maintain compliance and adapt to evolving regulatory standards post-authorisation.



# Contact us

**Marios Lazarou**
Board Member
Head of Advisory
**T:** +357 22 209 107
**E:** Marios.Lazarou@kpmg.com.cy

**Marie-Helene Angelides**
Senior Associate
Requlatory compliance, Risk Consulting
**T:** + 357 22 209 227
**E:** mangelides@kpmg.com

---

**Nicosia**
**T:** +357 22 209 000
**F:** +357 22 678 200
**E:** nicosia@kpmg.com.cy

**Limassol**
**T:** +357 25 869 000
**F:** +357 25 363 842
**E:** limassol@kpmg.com.cy

**Larnaca**
**T:** +357 24 200 000
**F:** +357 24 200 200
**E:** larnaca@kpmg.com.cy

**Paralimni**
**T:** +357 23 820 080
**F:** +357 23 820 084
**E:** paralimni@kpmg.com.cy

**Paphos**
**T:** +357 26 943 050
**F:** +357 26 943 062
**E:** paphos@kpmg.com.cy

**Polis Chrysochous**
**T:** +357 26 322 098
**F:** +357 26 322 722
**E:** paphos@kpmg.com.cy

**www.kpmg.com.cy**