



● Navigating the Markets in Crypto Assets Regulation (MiCAR)

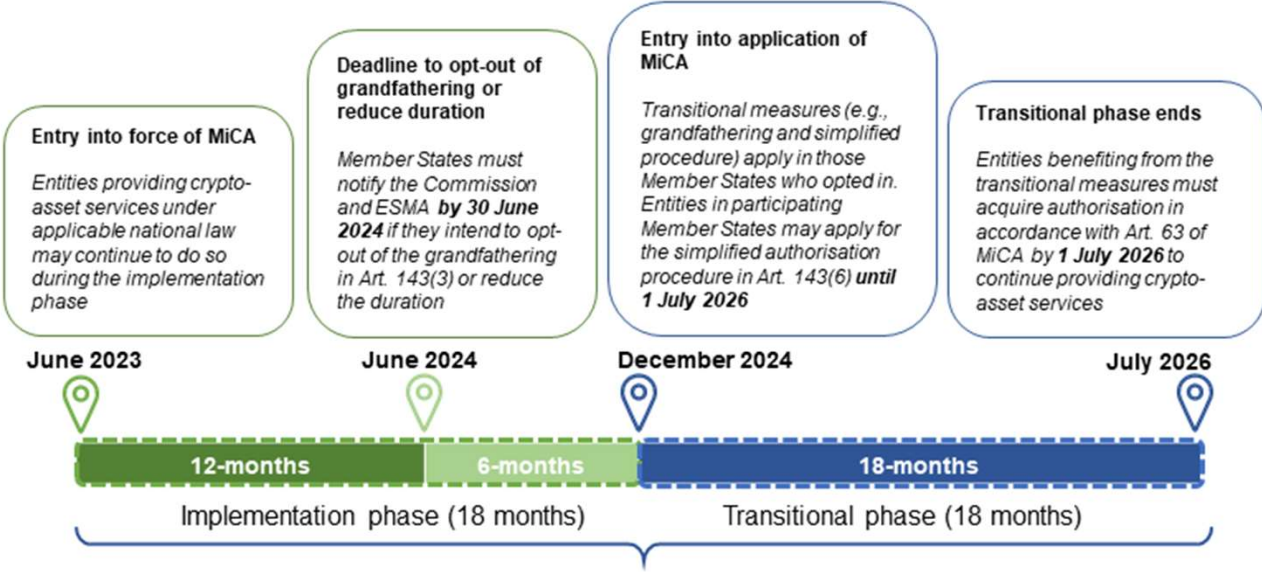
Preparing Your Crypto Business for Compliance

December, 2023

INTRODUCTION

- Markets in Crypto Assets Regulation (MiCAR) entered into force on 9 June, 2023.
- The new regulation for the crypto-asset market will be applied in **two stages**:
 - Part III (Asset-referenced tokens (**ARTs**)) and Part IV (Electronic money tokens (**EMTs**)) will come into effect from June 30, 2024;
 - The remaining provisions of MiCAR will be enforced starting December 30, 2024.
- MiCAR's **primary objective** is to regulate crypto-assets not covered by other EU financial services legislation and to oversee the activities of crypto-asset service providers.
- The following **service providers** will fall under the scope of MiCAR:
 - Issuers of crypto assets (Part II);
 - Issuers of ARTs (Part III);
 - Issuers of EMTs (Part IV);
 - Crypto-Asset Service Providers (**CASPs**) (Part V) (incl. crypto-assets exchanges, crypto-assets custody providers, crypto-assets trading platforms operators, and similar).
- These service providers will be obliged to obtain the **relevant licence**, which will be **passportable** across the EU. This means that a service provider based in one EU Member State (**MS**) will have the freedom to offer services across the EU, either on a freedom to provide services or freedom of establishment basis.

TIMELINE



MiCA 36-month timeline for entities already providing crypto-asset services

Transitional period:

MSs will have an option of **'transitional measures'** (Art. 143 of MiCAR) that would allow undertakings already providing crypto-asset services to **continue doing so** during the transitional phase of MiCAR. These transitional measures include:

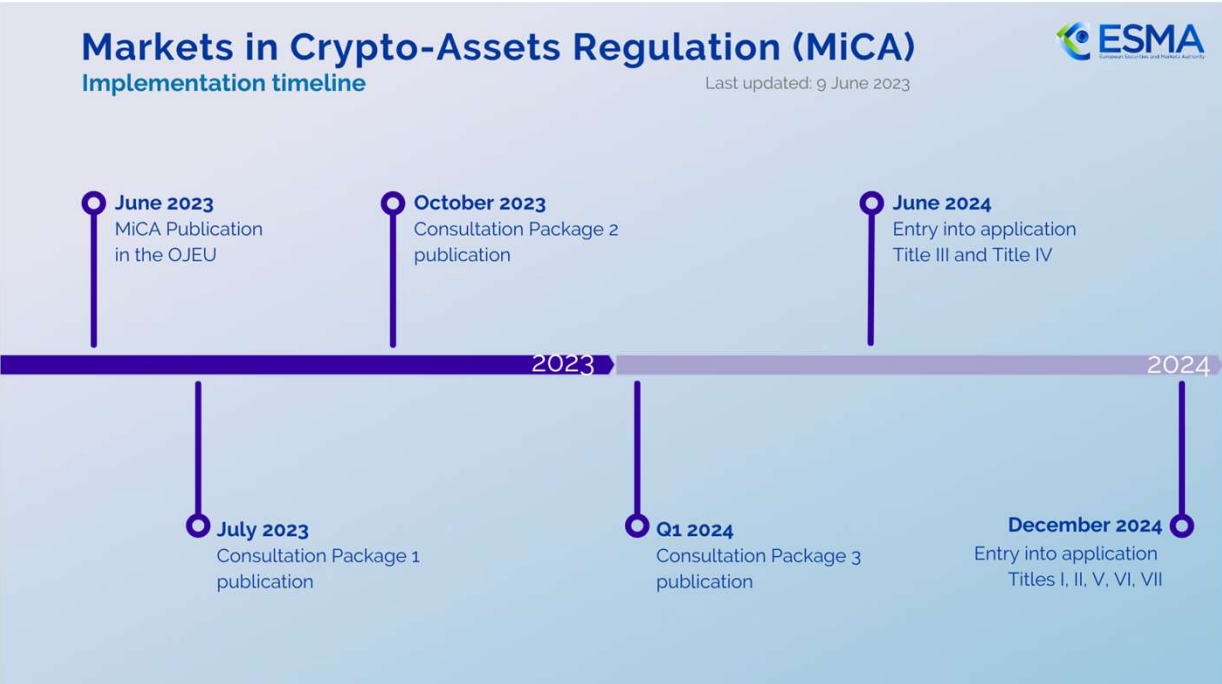
- **A 'grand-fathering' clause** – allowing entities providing crypto-asset services in accordance with national applicable laws before 30 December 2024 to continue to do so **until 1 July 2026** or until they are granted or refused a MiCA authorisation;
- **A simplified authorisation procedure** – for entities that were already authorised under national applicable law on 30 December 2024 to provide crypto-asset services.

MSs have to decide re **opt-out** of grandfathering clause/ reduce of the duration **until June, 2024**.

There is still no formal clarity re applicability of grandfathering clause in Lithuania.

TIMELINE

The scope and applicability of MiCAR are currently subject to some ambiguity and lack clarity.



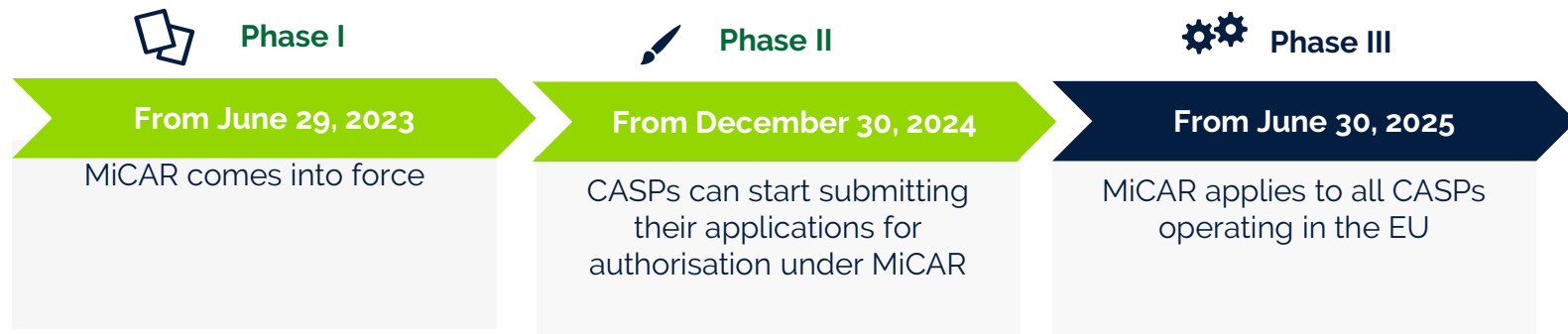
ESMA is releasing the **MiCAR consultation packages**, which provide/ will provide more clarity and detailed information on the requirements for obtaining a license for CASPs, governance, record-keeping, the qualification of crypto-assets as financial instruments, reverse solicitation, and more.

- The **first package** was launched in July 2023.
- The **second package** was launched in October 2023.

The third and final consultation package is expected to be published in **Q1 2024**.

TRANSITIONAL PERIOD FOR CASPs

The formal MiCAR timeline is as follows:



N.B. According to the latest communication from government authorities in Lithuania, there will be no transitional period. According to draft legislation, all CASPs will have to submit their applications for MiCA licence until 1st of July, 2024, and secure their licence until 30th December, 2024; otherwise, they will lose the right to provide services.

WHAT CHANGES?

01. Authorization: CASPs will need to be authorized by a national competent authority to operate in the EU. This process involves meeting specific requirements, such as establishing a robust **risk management framework** and ensuring the ability **to protect customer assets**. On **October 6, 2023**, it was announced that the Bank of Lithuania will assume the role of the competent authority issuing licenses under MiCAR in Lithuania.

02. Transparency: CASPs will need **to disclose** their customers with specific information, including details about the fees they impose and the risks associated with trading crypto-assets.

03. Customer protection: CASPs will be obliged to comply with requirements for remote marketing, contract conclusion, and complaints handling. CASPs providing advice on crypto-assets will **need to assess** whether those crypto-asset services or crypto-assets are suitable for their customers and others.

04. Market abuse: CASPs will be subject to market abuse rules, which are designed to prevent **insider trading** and **market manipulation**.

05. Regulatory requirements: MiCAR will also introduce a number of other requirements for CASPs, including rules on how they handle customer **deposits and withdrawals**, and how they manage **conflicts of interest**.



WHY EMBRACE IT?

02. Investor Protection: One of the primary goals of regulation is to protect investors from fraud, scams, and market manipulation. Regulations may require CASPs to **implement security measures**, conduct **due diligence** on token issuers, and provide **clear information** to investors.

04. AML/CTF/KYC and Sanctions Compliance: Regulation require CASPs to implement procedures for Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), Know Your Customer (KYC) and international sanctions **to manage risks** and **prevent illegal activities** such as money laundering, terrorist financing, sanctions evasion, etc.

01. Increased Legitimacy: Regulations can help legitimize the cryptocurrency industry in the eyes of traditional investors, institutions, and the general public. This can lead to **greater adoption and acceptance** of crypto-assets as a legitimate asset class.

03. Market Integrity: Regulations play a crucial role in ensuring **fair and transparent trading practices** in crypto markets. This involves implementing measures to prevent market manipulation, insider trading, and price manipulation.

05. Cross-Border Regulations: CASPs operate on a **global scale**, necessitating regulations that address cross-border issues, including **international coordination** on regulatory standards and enforcement.

BORDERS

How can one cross them?

- **EU Passporting:** CASPs shall be allowed to provide crypto-asset services throughout the EU, either through the **right of establishment**, including through a branch, or through the **freedom to provide services**. CASPs that provide crypto-asset services on a cross-border basis shall not be required to have a physical presence in the territory of a host MS.
- **Reverse solicitation:** Where a client established or situated in the EU **initiates at its own exclusive initiative** the provision of a crypto-asset service or activity by a third-country firm, the requirement for authorisation shall not apply to the provision of that crypto-asset service or activity by the third-country firm to that client, including a relationship specifically relating to the provision of that crypto-asset service or activity.





II. GETTING AUTHORISED

AUTHORISATION

What does it take?

- To obtain authorisation under MiCAR, CASPs will need to meet a number of **requirements** related to the applicant's readiness to manage risks, legal establishment in the EU, consumer protection and similar considerations.
- **Application** requirements and key focus areas are provided in the following slides.
- CASPs can submit their applications for authorisation under MiCAR **from December 30, 2024** (in **Lithuania**, discussions are underway about initiating the full licensing process even before the full applicability of MiCAR. The draft law indicates that CASPs registered in Lithuania may need to apply for a licence by June 30, 2024. Not yet confirmed).
- The national competent authority (Bank of Lithuania in Lithuania) will then **assess the application and decide** whether or not to grant authorisation. If the application is successful, CASP will be able to operate in the EU.
- It is important to note that the authorisation process under MiCAR is expected to be **rigorous and time-consuming**. Therefore, CASPs should start preparing their applications as early as possible.

APPLICATION | 1

1. Business information	Program of operations (incl. business plan, COI management, outsourcing arrangements and policy, other), proof of compliance with prudential safeguards requirements, description of governance arrangements, and proof of good repute and experience of management body members
2. Shareholder information	Identity of any shareholders and members with qualifying holdings , and proof of their good repute
3. Risk management	Description of internal control mechanisms, policies, and procedures to identify, assess, and manage risks , including money laundering and terrorist financing risks, and business continuity plan
4. Technical information	Technical documentation of ICT systems & security arrangements and a description thereof in non-technical language
5. Client asset & funds protection	Description of the procedure for the segregation of clients' crypto-assets and funds
6. Complaints handling	Description of the CASP's complaints-handling procedures
7. Custody and administration	Where the CASP intends to provide custody and administration of crypto-assets on behalf of clients, a description of the custody and administration policy
8. Trading platform	Where the CASP intends to operate a trading platform for crypto-assets, a description of the operating rules of the trading platform, procedure and system for detection of market abuse
9. Exchange of crypto-assets	Where the CASP intends to exchange crypto-assets for funds or other crypto-assets, a description of the commercial policy governing the relationship with clients and the methodology for determining the price of the crypto-assets
10. Execution of orders	Where the CASP intends to execute orders for crypto-assets on behalf of clients, a description of the execution policy
11. Advice & portfolio management	Where the CASP intends to provide advice on crypto-assets or portfolio management of crypto-assets, proof that the natural persons giving advice or managing portfolios on CASP's behalf have the necessary knowledge and expertise
12. Transfer services	Where the CASP intends to provide transfer services for crypto-assets on behalf of clients, information on the manner in which such transfer services will be provided
13. Type of crypto-asset	The type of crypto-asset to which the crypto-asset service relates

APPLICATION | 2

And...?

In addition, the CASP must also furnish proof of the following:

- **Good repute and experience of management body members:**
 - The **absence of a criminal record** or penalties imposed under applicable law for convictions related to anti-money laundering, counter-terrorist financing, fraud, or professional liability;
 - Collective possession of appropriate **knowledge, skills, and experience** by CASP management body members to effectively manage the CASP, along with a commitment of **sufficient time** to perform their duties;
- **Good repute of shareholders and members:**
 - The **absence of a criminal record** or penalties imposed under applicable law for convictions related to anti-money laundering, counter-terrorist financing, fraud, or professional liability for all shareholders and members with qualifying holdings in the CASP.



KEY REQUIREMENTS

Focus on?

- 1. Sound risk management framework**

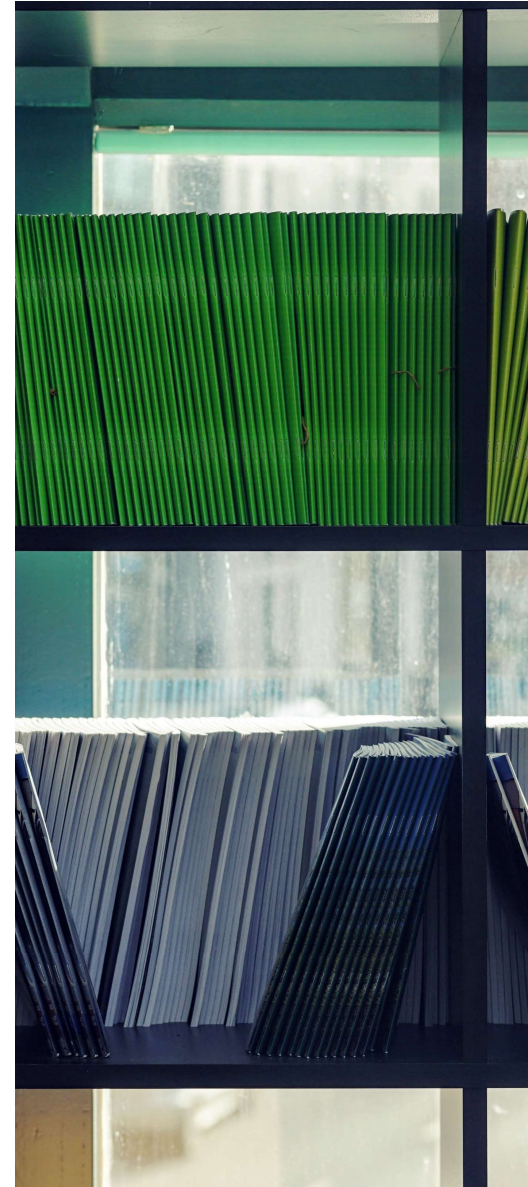
CASPs must establish an adequate risk management framework **to identify, assess, manage, and mitigate** the risks associated with their business. This framework must include policies and procedures for managing various risks, including market risk, operational risk, and credit risk.
- 2. Protection of customer assets**

CASPs must implement measures to safeguard customer assets from theft and loss. This involves practices such as storing customer assets in **secure wallets** and having appropriate **insurance coverage** in place.
- 3. Good reputation and financial standing**

CASPs must maintain a good reputation and financial standing. This requires them to demonstrate both **financial soundness** and a positive **track record** of compliance with regulations.
- 4. Qualified and experienced staff**

CASPs must ensure their staff comprises qualified and experienced professionals capable of **handling and managing the risks associated with the business**. This encompasses individuals with expertise in risk management, compliance, and cybersecurity.
- 5. Audit**

CASPs must be audited by an **independent auditor on an annual basis**. This is to provide assurance that CASPs are complying with all applicable laws and regulations, and that their financial statements are accurate.



SCOPE

Additional requirements for specific services



- | | |
|---|---|
| 1. CASPs that provide custody and administration of crypto-assets on behalf of clients must: | <ul style="list-style-type: none">• Segregate client assets from the CASP's own assets• Implement appropriate security measures to protect client assets, such as storing them in secure wallets and having insurance in place• Have adequate insurance in place to cover losses of client assets |
| 2. CASPs that operate a trading platform for crypto-assets must: | <ul style="list-style-type: none">• Have a fair and transparent trading platform• Prevent market abuse, such as insider trading and market manipulation |
| 3. CASPs that exchange crypto-assets for funds or other crypto-assets must: | <ul style="list-style-type: none">• Have a clear and fair pricing policy• Disclose all relevant information to customers before they enter into a transaction |
| 4. CASPs that execute orders for crypto-assets on behalf of clients must: | <ul style="list-style-type: none">• Obtain the best possible execution for their clients' orders• Have adequate risk management systems in place• Prevent market abuse, such as insider trading and market manipulation |
| 5. CASPs that place crypto-assets must: | <ul style="list-style-type: none">• Have a clear and transparent admission policy• Disclose all relevant information to investors before they invest |
| 6. CASPs that receive and transmit orders for crypto-assets on behalf of clients must: | <ul style="list-style-type: none">• Transmit orders accurately and promptly• Have adequate risk management systems in place |
| 7. CASPs that provide advice on crypto-assets must: | <ul style="list-style-type: none">• Act in the best interests of their clients• Provide suitable advice to their clients, taking into account their individual circumstances• Disclose all relevant information to their clients before they provide them with advice |
| 8. CASPs that provide portfolio management of crypto-assets must: | <ul style="list-style-type: none">• Act in the best interests of their clients• Manage their clients' portfolios in accordance with their clients' investment objectives and risk tolerance• Disclose all relevant information to their clients before they manage their portfolios |

DON'TS

What can't one do?

The following crypto-related services are *not allowed* under MiCAR:

1. Offering or selling crypto-assets that are classified as securities under MiFID II	This includes crypto-assets that represent ownership in a company, such as security tokens
2. Offering or selling crypto-assets that are classified as derivatives under MiFID II	This includes crypto-assets that are linked to the price of another asset, such as Bitcoin futures
3. Managing crypto-assets on behalf of customers in a discretionary manner	This means that the CASP would be making investment decisions on behalf of its customers without their prior consent

Note: Some countries in the EU may impose additional regulations restricting the provision of crypto-related services. For instance, certain countries have prohibited the use of anonymous cryptocurrencies, such as Monero. CASPs should, therefore, verify the regulations in the countries where they operate to ensure compliance.

THE LARGEST TEAM OF LAWYERS IN THE BALTICS

THE LARGEST TEAM

250+ lawyers with top competences, including 49 partners in the Baltics, working in an integrated manner in specialised teams across all business sectors.

[Meet our experts](#)

INNOVATION IN LAW

In the [index](#) of 2022, the prestigious business awards FT Innovative Lawyer nominated Ellex among TOP40 most innovative European law firms. Ellex was recognised for its innovations in law, including the creation of the AML risk assessment tool [Goolkit](#) and the digital health consultation platform [Viveo Health](#).

In 2018, Ellex was the first Baltic law firm included by the Financial Times in the index of the most innovative law firms for using artificial intelligence to provide optimized legal services.



The Ellex team was the first in the Baltic states to begin developing the [#EllexDigital](#) project designed to provide specialised legal assistance on IT-related matters. The project also embraces an educational initiative to train the business community on the digitalisation challenges in law.

EXCLUSIVE KNOWLEDGE FROM WORLDWIDE NETWORKS

Member
LexMundi
World Ready



WSG
World Services Group

ENERGY LAW GROUP

INTERNATIONAL AWARDS AND RECOGNITIONS



IFLR1000
WOMEN LEADERS

WOMEN IN BUSINESS LAW AWARDS 2022 EMEA

FT INNOVATIVE LAWYERS



Ellex[®]
Experience success

Ellex[®] Raidla

Roosikrantsi 2,
EE-10119 Tallinn, Estonia
+372 6407170
+372 6407171
contact@ellex.ee

Ellex[®] Klavins

K.Valdemara 62,
LV-1013 Riga, Latvia
+371 67814848
+371 67814849
contact@ellex.lv

Ellex[®] Valiunas

Jogailos g. 9,
LT-01116 Vilnius, Lithuania
+370 52681888
+370 52125591
contact@ellex.lt