KPMG Law

# Regulation for Crypto-Asset Service Providers

MiCAR:
A Sea Change
in Regulation

kpmglaw.ie

# Regulation for Crypto-Asset Service Providers

## MiCAR: A Sea Change in Regulation

The crypto-industry has been at the forefront of innovation in both retail and business services; seeking to provide alternative solutions to existing traditional financial services. Whilst this has successfully generated significant new opportunities, products and wealth, issues in terms of consumer protection, security, financial stability, and governance have emerged in what is generally an unregulated space.

The Markets in Crypto-Assets Regulation **(MiCAR)** represents a sea-change in the regulation of crypto-asset service providers **(CASPs)** in the EU, bringing with it many challenges for existing operators who have to date avoided the full scope of financial regulation.

The downfall of operators such as OFX demonstrate the gulf between the approach of crypto-firms and the needs and expectations of regulated financial service providers in other markets. Existing operators will therefore need to get to grips with a significant shift in how they operate and do business, both from an organisational and compliance perspective. The move from the unregulated to the regulated space will therefore require significant uplift for existing operations; importing many aspects of financial regulation supervision, oversight and management, including rules on: corporate governance; capital requirements; conduct of business; financial crime; and outsourcing and operational resilience.

These new requirements will ultimately bring CASPs fully within the regulatory perimeter; with all of the associated oversight and challenges.

With the imminent implementation of MiCAR and the need for CASPs to submit authorisation applications, how can new and existing firms best prepare?

Lessons can be learnt from the evolution of financial regulation and supervision in other sectors, as well as the ever-evolving approach of regulators both in Ireland and across the EU. Whilst there has been much discussion of the precise rules under MiCAR, what will regulation mean in practice for firms, and where do they need to best focus their resources and effort to ensure compliance and meet regulators' expectations?

These requirements do not necessarily derive directly from MiCAR, but instead apply to all regulated entities. It is therefore important to consider both MiCAR and other regulatory requirements more generally as they will apply to CASPs.

Although MiCAR includes broader requirements on issuers of crypto-assets, and specific requirements relating to certain assets, such as stablecoins, this papers seeks to focus on the particular regulatory and governance issues facing CASPs, which will need to understand the consequences and challenges of becoming fully authorised regulated financial service providers, subject to the on-going supervision and oversight of regulators such as the Central Bank of Ireland **(Central Bank)**.

# Corporate Governance

## Registered Office in the EU

The decentralised nature of crypto-assets and the global nature of service providers has meant that EU customers have, to date, been serviced by firms operating all over the globe, with limited, if any, physical presence within the EU. MiCAR effectively requires all CASPs looking to provide services to customers in the EU (and EEA) to establish a registered office in a Member State in order to obtain authorisation under MiCAR. Some level of solicitation of local customers would, however, be required, and MiCAR recognises that where services are provided on a reverse solicitation basis / at the client's own initiative, this will not trigger a need for local authorisation.

In Ireland, the establishment of a company is generally a straightforward process and can be completed quickly through registration with the Companies Registration Office. From a practical perspective, this is not a significant undertaking. However, it is important to understand that as for other types of regulated entity it will be this company, once authorised, which will be expected to 'own' the legal and regulatory requirements under MiCAR, and will need to be the 'mind and management' of the CASP in the EU. This means that the day-to-day decisions about the direction of the business will need to be taken by the directors and management of this company. Although regard can be had to group approaches and their international implementation, regulators will require that the business is ultimately run by the directors and management of this entity, and not group boards or individuals located in third country such as the US or UK.

This requirement also means that the use of Decentralised Autonomous Organisations (DAOs) for CASPs will not be permissible.

## Board Structure

MiCAR requires CASPs to have at least one director resident in the EU. However, in practice, at least in Ireland, it is likely that in order to ensure the mind and management of company is in Ireland, as well as for tax reasons, a majority of the board will need to be locally resident.

In terms of composition, it is expected that a minimum of three directors will be needed on the board, with a majority of non-executive directors. The need for non-executive directors, and particularly independent non-executive directors (INEDs) is seen by the Central Bank as being a fundamental part of effective corporate governance. The role of the INED in regulated entities is to provide independent challenge on boards; bringing an independent viewpoint to the deliberations of the board that is objective and independent of the activities of the management. The chair of the board will also need to be a non-executive director.

At a minimum, it should therefore be expected that the board would be comprised of an executive director / chief executive officer, at least one INED, and another non-executive director (either an INED or a group non-executive director). It is also possible that for potentially larger or systemically important CASPs the Central Bank could seek a larger board, with additional executive and/or non-executive directors, to ensure effective governance in light of the nature, scale and complexity of the firm's business.

## Key Senior Management

In addition to a board, firms will be expected to have a number of key functions. Although the precise roles are not prescribed, in line with other regulated entities, these will likely include: Head of Finance / Finance Director, Head of Compliance, Head of Anti-Money Laundering and Countering the Financing of Terrorism **(AML/CFT)**, Head of Risk, Chief Operating Officer, Head of Internal Audit, and Chief Information Officer / Chief Technology Officer.

Depending on the nature scale and complexity of the firm's business, it may be possible to dual-hat some of these functions (i.e. one individual may carry out more than one role) and/or to outsource certain of these functions to third party providers or group functions. However, the overarching requirement to ensure that the mind and management of the firm remains within the firm will need to be borne in mind.

## Fitness and Probity: Pre-Approval Controlled Functions

MiCAR includes a general requirement to ensure that all members of the management body of a CASP are of sufficiently good repute and possess the appropriate knowledge, skills and experience, both collectively (i.e. when viewed holistically across all members) and individually. There is also a requirement to ensure that the CASP more generally employs personnel with the knowledge, skills, and expertise necessary for the discharge of responsibilities allocated to them.

In Ireland, these requirements are also more generally reflected in the Central Bank's Fitness and Probity regime. This includes a requirement for all regulated entities to obtain prior approval from the Central Bank for certain key management positions (referred to as Pre-Approval Controlled Functions **(PCFs)**). This will include all directors as well as all of the key senior management functions listed above.

All PCFs will be assessed by the Central Bank for both fitness (i.e. their ability, knowledge and competence to carry out the relevant role) and probity (i.e. their honesty, integrity, and financial soundness). PCFs are required to complete individual questionnaires providing details of the professional background, and any issues which could impact on their probity (for example whether they or firms in which they have had previous involvement have been the subject of regulatory investigations or fines, or have been subject to criminal sanctions). The PCF assessment will be carried out by the Central Bank in parallel with the authorisation application.

Once authorised, it will be necessary to obtain the Central Bank's prior approval for any proposed new appointments. It will therefore be important to ensure that appropriate succession planning is in place to avoid situations where one or more of the above board or senior management functions becomes vacant.

## Individual Accountability Framework

The Central Bank has recently implemented an Individual Accountability Framework (IAF) applicable to all regulated entities, with the aim of enhancing the governance and culture in regulated firms. Firms will need to identify how the business and its risks are being managed, and the specific individuals responsible.

The IAF Introduced Common Conduct Standards for all person subject to fitness and probity requirements (including both PCFs (discussed above) as well as persons carrying out certain other controlled functions), and Additional Conduct Standards for certain senior management.

These conduct standards will need to be embedded within a firm's broader governance structure and culture, as well as employment contracts and processes.

The IAF also introduced a Senior Executive Accountability Regime **(SEAR)**, under which certain senior management had a duty to take reasonable steps to prevent the firm from committing regulatory breaches. The SEAR is being introduced on a phased basis from 1 July 2024. CASPs will not be included in the categories of regulated entities impact under the initial phase of SEAR, but may be included in subsequent phases. Notwithstanding, many of the elements required under SEAR, including identifying areas of responsibility and management responsibility mapping, are useful guides to good corporate governance. CASPs may therefore wish to consider which elements of SEAR may assist in meeting general good corporate governance requirements.

## Three Lines of Defence

Regulated entities are expected to employ the so-called 'three lines of defence' model to compliance. The three lines are:

**First Line:** The people who have responsibility for complying with regulatory requirements and policies on a frontline basis (e.g. executive management and frontline staff).

**Second Line:** Those responsible for the oversight of the first line (i.e. the compliance and risk functions).

**Third Line:** The audit function, which oversees both the first and second lines.

In order to ensure an effective compliance framework, regulated firms are required to ensure that there is operational independence between the three lines. In practice this means that persons performing a function in one line of defence cannot also carry out a role in another. Thus, a person responsible for day-to-day management of the firm could not also have a role in the compliance or risk functions, and similarly a person working the compliance function could not have a role in the audit function. This is to prevent conflicts of interest arising within the compliance framework, i.e. to effectively ensure that people are not 'marking their own homework'.

Accordingly, as noted above, whilst it may be possible for certain individuals to carry out more than one role within a firm, it will not be possible for individuals to dual-hat roles from different lines of defence (e.g. the Chief Operating Officer could not also be the Head of Risk or Internal Audit). This will therefore need to be taken into account in the firm's resource planning and management.

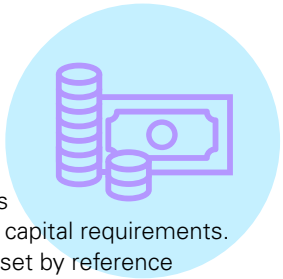
## Shareholders in CASPs

Shareholders in CASPs will be subject to assessment by the Central Bank in a similar manner to other regulated entities. MiCAR includes a requirement that shareholders with qualifying holdings (i.e. at least 10% direct or indirect capital or voting rights) must be of sufficiently good repute, and particularly must not have been convicted of money laundering or terrorist financing (or any other convictions impacting on their repute).

All qualifying shareholders will need to be assessed by the Central Bank as part of the initial authorisation, and any new qualifying shareholders will need to go through the acquiring transaction process. Increases in qualifying shareholdings above certain thresholds (namely 20%, 30% or 50%) will similarly require the Central Bank's non-objection. Disposals of qualifying shareholdings, or where one of the thresholds is crossed as a result of a disposal, will need to be notified to the Central Bank.

It should also be noted that if the Central Bank considers that shareholders could exercise influence *"likely to be prejudicial to the sound and prudent management"* of the CASP, it is required by MiCAR to take appropriate measures to address those risks. Such measures could include judicial orders, the imposition of penalties against directors or management, or the suspension of the voting rights of the shareholder. This requirement derives from the need for the CASP and its management to be ultimately responsible for the day-to-day management of the business. It is also likely that in the event that shareholders were found to have exercised influence which could be prejudicial to this, that the overall corporate governance and management structure of the CASP will draw on-going supervisory focus to ensure that such influence does not, in practice, continue or resurface.

# Capital Requirements



As for many regulated entities, CASPs will be subject to initial and minimum capital requirements. The level of initial minimum capital is set by reference to the proposed crypto-asset services to be provided: CASPs providing execution, placing, transfers, receipt and transmission, advice or portfolio management will have a minimum capital requirement of €50,000; CASPs providing custody and exchange services will require €125,000; and CASPs operating a trading platform will require €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.

In order to meet these requirements, CASPs will need to either hold own funds (consisting of Common Equity Tier 1 items as set out in the Capital Requirements Regulation), and/or to put in place an insurance policy for this amount. The insurance policy will need to provide cover against the risk of loss of documentation, misrepresentations or misleading statement, acts, errors or omissions resulting in breaches, failures relating to conflicts of interest, losses arising from business disruption or systems failures, gross negligence in safeguarding clients' crypto-assets and funds (where relevant) and liability towards clients for loss of assets.

# Conduct of business

One of the key drivers of MiCAR was the experience of consumers who were being exposed to significant risks from "investments" in crypto-assets. Whilst Bitcoin was initially touted as primarily a decentralised payment system, its volatile (and increasing) value attracted many people looking to purchase it as an investment, rather than for the purpose of making payments. This created similar risks for consumers as with other types of investment products, such as shares, but in a generally unregulated market.

Further, although initial speculators may have been on the more 'tech-savvy' side, often using self-custody, as more traditional consumers moved into the market, service providers increasingly sought to provide both transactional services and custody, intermediating between consumers and market makers, again moving towards more traditional models of financial services, such as investment firms.

With the increase in services, as well as risks, and a number of high-profile failures and frauds, it was inevitable that regulations similar to the Markets in Financial Instruments Directive **(MiFID)**, the Payment Services Directive, and the Prospectus Regulation (in respect of issuers) would arise.

MiCAR therefore includes a number of key conduct of business measures for CASPs, including:

- **Consumer protection:** This includes general requirements to act honestly, fairly and professionally in the best interests of clients, and to ensure that information and marketing is fair, clear and not misleading, as well as requirements around complaints handling. These are similar to the existing provisions of the Consumer Protection Code and aim to mitigate the risk to consumers and smaller businesses when dealing with financial service providers.

- **Transparency and Disclosure requirements:** CASPs will be required to have in place agreements with clients outlining the nature of the services to be provided, the fees, costs and charges, and various other prescribed matters and policies (depending on the services being provided), as well as associated policies and procedures. These aim to ensure that customers are provided with clear and transparent terms relating to the services, as well as the policies and procedures in place to protect customers and their assets.

- **Client asset protections:** Similar to both client asset requirements for investment firms, and safeguarding requirements for payment and e-money institutions, CASPs will be required to segregate and safeguard client crypto-assets and funds. This will seek to ensure that in the event of a CASP's insolvency crypto-assets and funds held by the CASP in connection with its services will be both identifiable and protected. In particular, CASPs will be required to ensure that they have adequate arrangements to safeguard the ownership rights of clients and prevent the use of clients' funds for their own account (something which was notably absent in the case of FTX, which used client assets to fund the owner's trading firm, Alameda Research). Similarly, any client funds (i.e. money provided by clients in connection with services) held at the end of the business day following receipt of the funds (T+1) will need to be placed with a credit institution or central bank, and held in accounts segregated from the funds of the CASP. Whilst not expressly stated in MiCAR, periodic reconciliation of the assets held on behalf of clients is also likely to be necessary to ensure that these obligations are met, and that there is clear identification and segregation of crypto-assets and funds held on behalf of a client.

- **Conflicts of interest:** As for investment firms, the nature of CASPs' services can potentially create conflicts of interests between the CASP, its management body, its employees, and its clients. CASPs are therefore required to implement and maintain effective policies and procedures to identify, prevent, manage and disclose potential conflicts of interest. The general nature and sources of potential conflicts of interest will need to be displayed in a prominent place on a CASP's website and disclosed to clients and prospective clients. These will need to be kept under review, at least annually, in order to ensure that all relevant conflicts are captured.

- **Market abuse:** The potential for insider trading and other market manipulation by CASPs is a significant risk to customers, as well as the broader market in crypto-assets. MiCAR has therefore introduced specific rules for crypto-assets admitted to trading (or that have been requested to be admitted to trading), irrespective of whether the trades take place on or off of a trading venue. These rules closely follow those already in place for listed securities and require the disclosure of inside information, prohibit insider dealing, and prohibit market manipulation (e.g. through the disclosure of false or misleading information relating to a crypto-asset's demand or price). CASPs will be required to have in place appropriate systems and procedures to prevent and detect potential market abuse and will need to report suspicions of market abuse to the Central Bank.

# Financial Crime

## Money Laundering and Terrorist Financing

A key driver in the regulation of CASPs has been the potential misuse of crypto-assets to facilitate money laundering and/or terrorist financing, and to circumvent financial sanctions. For this reason, a registration regime for virtual-asset service providers **(VASPs)** (broadly equivalent to CASPs) was introduced as part of the Fifth Money Laundering Directive in advance of MiCAR. This was to ensure that service providers were clearly captured by the obligation to put in place appropriate measures to prevent and detect money laundering and terrorist financing, including carrying out customer due diligence, monitoring transactions, and putting in place policies and procedures to support this. Notwithstanding, there has been significant divergence in the approach to the registration process across the EU, with some Member States using a light-touch registration process, and others (including Ireland) making the process almost akin to a full authorisation. The MiCAR authorisation process for CASPs should eliminate this divergent approach.

Existing VASPs/CASPs should therefore already have developed AML/CFT processes and procedures, but it should be expected that additional scrutiny will be placed on these controls as part of the authorisation process, and on an on-going basis going forward, as regulators continue to see the sector as being exposed to a high risk of money laundering and terrorist financing.

## Information to Accompany Transfers of Crypto-Assets

In addition to general AML/CFT requirements, there are also requirements under the Funds Transfer Regulation, which currently requires certain information on payers and payees to accompany transfers of funds for the purposes of preventing money laundering and terrorist financing, that are to be expanded to include transfers of crypto-assets, including transfers *"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."*

The CASP of the beneficiary (i.e. the person to whom the transfer is being made) will also be required to have in place systems to detect missing information which should have accompanied the transfer, and to verify the information on the beneficiary. If missing information is identified, the beneficiary's CASP will be required to either reject the transfer or to take steps to obtain the information from the originator's CASP before making the crypto-assets available. If a CASP repeatedly fails to include the required information, the beneficiary CASP will be required to warn the originating CASP, reject any future transactions from the CASP, and inform the Central Bank (or other competent authority). Suspicious transactions reports may also need to be filed with the Financial Intelligence Unit of An Garda Síochána and the Revenue Commissioners.

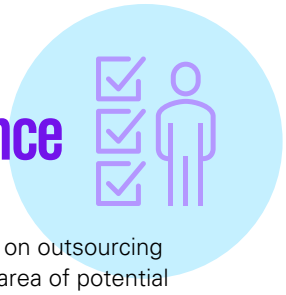
CASPs will therefore need to ensure that their systems facilitate these requirements both when sending and receiving transfers of crypto-assets.

## Financial Sanctions

It is also important to note that financial sanctions (such as those currently imposed in respect of the Russian invasion of Ukraine) will also need to be complied with (as for all EU persons). CASPs will therefore need to ensure that they have appropriate systems and controls in respect of customers and transactions to ensure that they are not used to facilitate payments to sanctioned persons or entities, or otherwise circumvent the relevant sanctions. Further, specific provision has already been made as part of the EU financial sanctions packages against Russia in relation to crypto-asset wallets, accounts, or custody services, which are expressly prohibited from being provided to Russian nationals, or natural persons residing in Russia, or to legal persons, entities or bodies established in Russia.

Breaches of financial sanctions (for example sending assets to a sanctioned person) are generally strict liability offences (i.e. there is no requirement to prove that a person intended to provide assets to a sanctioned person in order to attract criminal liability). Notwithstanding, liability can be avoided where a person can demonstrate that *"they did not know, and had no reasonable cause to suspect"* that their actions would result in a breach of financial sanctions. However, this defence is interpreted narrowly. It is therefore it is important that firms which have the potential to breach financial sanctions (particularly those in financial services) are able to demonstrate that they had in place appropriate systems and controls around financial sanctions to prevent breaches. Appropriate sanctions screening procedures will therefore be important for CASPs to mitigate against the risk of breaches of financial sanctions.

# Outsourcing and Operational Resilience



## Outsourcing

Regulators have increasingly focussed on outsourcing and operational resilience as being an area of potential risk from a governance and compliance perspective. Having in place appropriate outsourcing frameworks and contractual arrangements is therefore important to ensure that where elements of service provision and back office support are not within a regulated entity, the firm can be confident that its outsource service providers are operating in a compliant manner, as ultimately it will be the regulated entity which will bear responsibility for any failures by its outsourced service providers.

MiCAR includes specific provisions on outsourcing by CASPs which generally reflect existing practices and expectations already applicable to other regulated entities. In particular, this includes requirements that the outsourcing does not result in the delegation of responsibility, does not alter the relationship between CASPs and their clients, does not impact on the ability of regulators to effectively exercise their supervisory functions, and that CASPs have direct access to relevant information on the outsourced services.

CASPs in Ireland will be subject to the Central Bank's Cross-Industry Guidance on Outsourcing, and will therefore need to ensure that their internal governance and oversight frameworks, as well as contractual arrangements with outsourced service providers, meet Central Bank expectations and requirements. This may necessitate engagement with these service providers to ensure that the CASP, its auditors, and the Central Bank, will have ready access to information on any outsourced services or activities, and that this is reflected in contractual arrangements with the providers. CASPs will also need to be conscious of any sub-outsourcing by their providers, and make sure that similar access to any sub-providers is also included.

CASPs will need to put in place appropriate policies, procedures, systems and controls to manage outsourced services and activities, with a particular focus on supervision and oversight of the activities through clear reporting lines, key performance indicators, and regular testing and challenge. Both the Chief Operating Officer as well as the Chief Technology Officer / Chief Information Officer will play key roles in this regard, and they should anticipate the actions they take concerning outsourced services and activities will be important consideration in any assessment of their compliance with their obligations under the IAF.

## Operational Resilience

In addition to general outsourcing requirements, operational resilience has been a significant focus from both the Central Bank and at an EU level. Operational resilience is the ability of firms, as well as the financial services sector as a whole, to prepare for and deal with operational disruptions. Although disruptive events may occur, these must be planned for and managed effectively to ensure that a firm is able to recover critical or important services, as well as protect customers and the broader financial system.

The Central Bank has produced its own Cross Industry Guidance on Operational Resilience, which sets out expectations with respect to the design and management of operational resilience, emphasises board and senior management responsibilities around operational resilience as part of risk management and investment decisions, and requires boards and senior management to take actions to ensure their frameworks are well-designed, robust, and operate effectively.

At an EU level, similar requirements are also set out in the Digital Operational Resilience Act **(DORA)** which is due to be implemented from the beginning of 2025. This is slightly narrower than the Central Bank's guidance (as it is limited to digital operational resilience), but will be particularly relevant to CASPs given their online business and operating models. DORA will necessitate putting in place certain measures to manage and mitigate against digital operational risks, and includes requirements in respect of contracts with third party service providers.

### WHAT'S NEXT?

New CASPs will need to apply for authorisation from 1 January 2025.

For existing CASPs already operating in accordance with national laws, a transitional period of 12 months has been provided and will run until the end of December 2025. These CASPs should however prepare applications for authorisation and engage with the Central Bank prior to the end of that period, as CASPs subject to the grandfathering provisions will not benefit from passporting rights (i.e. the ability to provide services on a cross-border basis across the EEA) until they are fully authorised.

# How we can help

KPMG has significant experience assisting regulated firms with all stages in a firm's lifecycle, from initial business planning, through authorisation and beyond.

Our multi-disciplinary teams including consultants, accountants, and lawyers allows us to provide unparalleled service through a single provider.

We can assist with both the authorisation application, as well as the implementation of policies, procedures and operational matters to ensure that firms are fully compliant with their legal and regulatory obligations, and can effectively navigate the authorisation process with the Central Bank.

Feel free to contact any of our specialists and advisors for more information on how we can assist.

# Contact us


**Christopher Martin**
Partner
Financial Services Regulation
KPMG Law LLP Ireland

**e:** christopher.martin@kpmglaw.ie

**Derek Hegarty**
Partner
KPMG Law LLP Ireland

**t:** +353 87 111 5982
**e:** derek.hegarty@kpmg.ie

**Ian Nelson**
Partner
KPMG Ireland

**e:** ian.nelson@kpmg.ie

**Matt Green**
Managing Director
KPMG Ireland

**e:** matthew.green@kpmg.ie

**Nicole Walsh**
Director
KPMG Law LLP Ireland

**e:** nicole.walsh@kpmglaw.ie

**David McMunn**
Director
KPMG Law LLP Ireland

**e:** david.mcmunn@kpmglaw.ie


**kpmglaw.ie**




Produced by: KPMG's Creative Services. Publication Date: May 2024. (10360)