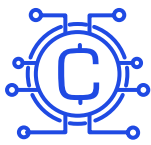




Safeguarding Consumers: Preparing for MiCA Regulation

June 2024





Introduction

This article delves into the consumer protection requirements under the Markets in Crypto-assets (MiCA) regulation, with a focus on the expectations of Crypto-Asset Services Providers (CASPs).

Firms aiming to capitalise on the growing interest in cryptocurrencies and blockchain technology need to consider these regulations carefully to ensure readiness and compliance. With critical timelines fast approaching, firms should ensure timely and comprehensive preparation to meet license and operating requirements in the short and long term.

In the past, the legislative framework surrounding cryptocurrencies varied extensively across the European Union. The absence of a unified approach resulted in a fragmented landscape with varying degrees of regulatory oversight. The introduction of MiCA has created a harmonised set of rules and expectations across member states. It aims to enhance consumer and investor protection, provide legal clarity, and ensure financial stability for those involved in crypto-asset transactions. The regulation defines a “crypto-asset” as a digital representation of value or rights that can be electronically transferred and stored using distributed ledger technology or similar innovations.

As the MiCA regulation extends to crypto-asset service providers (CASPs), firms should consider their involvement in crypto-asset activities and if they are within scope of the regulation. CASPs include firms who operate platforms and exchanges, setting clear expectations for how they are ensuring the safeguarding of consumer and investor interests and contributing to the upholding of market integrity.

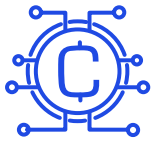
MiCA requires CASPs to apply for authorisation to operate within the European Union. CASPs requiring this authorisation includes those engaged in public offerings and trading activities, wallet providers, exchanges, in addition to those offering services relating to custody and administration of crypto-assets. By

encompassing asset, market and service providers that previously operated outside the regulatory scope, MiCA is set to establish a level playing field for those with an interest in crypto-asset markets.

From a consumer protection perspective, the regulation sets clear rules on the provision of information, timely disclosure, fraud protection, transparency, and fairness. These requirements mandate the clear and comprehensive information about the services and products offered, reducing the risk of fraud and unethical practices, while promoting consumer and investor interests. Notably, compliance is not just about meeting regulatory standards; it is about upholding fundamental principles of fairness, transparency, and market integrity.

Throughout this article, we will delve into how MiCA embodies essential consumer protection principles and explore its implications for the integrity and sustainability of the crypto market. By examining MiCA’s consumer protection measures, particularly in terms of transparency, disclosure, and advertising requirements for CASPs, we aim to illuminate the regulatory environment and the expectation on firms who operate within crypto-asset markets.





Consumer Protection under MiCA Regulation



Fairness

MiCA prohibits unfair practices, such as misleading advertising or deceptive marketing tactics, aligning with its overarching objectives to promote market fairness and investor confidence.

Fairness in the crypto market means setting standards for the issuance and trading of crypto-assets, ensuring all participants have equal access to information and opportunities. MiCA also requires firms to implement measures to safeguard the interests of novice investors and individuals with limited financial literacy.



Safeguarding

Firms must prioritise the best safeguarding of customers and investors, promoting a secure and accessible digital economy. They should ensure consumer and investor interests are considered throughout product and services lifecycles and be able to clearly demonstrate solid custody and safekeeping measures.

The regulation contains specific rules regarding safeguarding including data protection, account segregation, fraud protection, in addition to less prescriptive expectations. CASPs should consider a multi-faceted approach to safeguarding, combining elements such as security protocols, compliance, investor protection, transparency and resilience to ensure robustness.

All CASPs, including those operating exchanges or platforms will need to fully consider and account for user interests. They should be able to demonstrate risk management practices that go beyond mere compliance and align with the spirit of the regulation. As crypto-markets are often volatile and investor maturity varies, cooling-off periods, redress and enhanced disclosures should be considered of to support these interests.



Accuracy

Accuracy in information disclosure is crucial. Investors need relevant, truthful information about the assets they are buying, selling or holding. The information provided must effectively support investors and consumers in understanding the risks, the operational mechanisms of the assets and the market dynamics.

MiCA emphasises the need for clear and accurate disclosure of product features and risks to investors. Firms who implement robust marketing and product governance will reduce the opportunity for errors in communications, advertising campaigns and product information.



Risk Management

As the cryptocurrency market is inherently volatile, firms should ensure robust risk management practices are in place to prevent and detect fraud, cyber-attacks, and market manipulation. Risks should be documented with associated controls, and clear lines of defence to provide assurance on the completeness and effectiveness of those controls. Information security risks should be assessed comprehensively with proactive monitoring to ensure prompt risk response.

In addition to risks relating to prudential requirements, CASPs should be prepared to demonstrate how they manage risks relating to consumer protection, market conduct, transparency, disclosure, governance, marketing, and suitability amongst others.



Governance

Effective governance is essential to ensure a safe and diverse digital economy that balances innovation with market integrity. This involves implementing clear oversight to prevent insider trading, unauthorised disclosure of confidential information, and market manipulation in relation to crypto-assets.

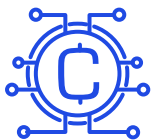
CASPs should implement ongoing monitoring and processes to ensure compliance with regulation and requirements. Necessary adjustments should be made to address any emerging challenges in a timely manner.



Risk Culture

MiCA introduces requirements which are relevant to many front-line and back office CASP employees, including those involved in marketing, selling and customer services. Entities should ensure a strong risk culture is in place to ensure all personnel understand and comply with obligations under the new regulation.

Firms should set clear tone from the top and consider internal messaging on the importance of identifying, reporting, and responding practices that could undermine market integrity.



What Does This Mean for Firms?

Entities providing or intending to provide crypto-asset services need to consider their consumer protection obligations carefully. They will be required to have a comprehensive knowledge of concepts and requirements covered under MiCA, including expectations relating to conduct, operating and prudential requirements. CASPs will also be required to be compliant with licencing, operating and conduct requirements, including:

Conflicts of Interest: Firms need to identify and address conflicts of interest arising from their business activities.

Marketing and Information Disclosures: Firms must ensure that marketing materials and disclosures are clear, fair, and free from ambiguous or misleading information. This includes providing accurate information on risks and potential returns of crypto investments and disclosing conflicts of interests.

Complaints Handling: Firms should ensure they have clear, effective procedures for handling client complaints in a transparent and timely manner. This involves expectations to identify and investigate complaints, explain the process clearly to customers, and retain adequate records regarding complaint decision and resolutions.

Outsourcing and Risk Management Practices: Firms must have robust risk management practices to identify, assess and mitigate risks associated with their operations. This includes conducting regular risk assessments, implementing appropriate controls, and establishing contingency plans for unforeseen events.

Additionally, firms should consider how consumers and investors engage and use their services as well as how to serve their interests across these touchpoints. Consideration of **conduct risk, fraud risk, market abuse** and **consumer protection** will vary depending on investor types and services offered. For example:

Custody and Administration of Crypto-Assets: Firms must have a deep understanding of the obligations to securely store and managing

digital assets for clients. This includes implementing strong security measures like multi-signature wallets, cold storage solutions and insurance coverage against theft or loss.

Operation of Trading Platforms and Exchange Services: Firms operating crypto exchanges must comply with rules on transparency, fairness and market integrity. This includes implementing measures to prevent market manipulation, ensure adequate liquidity and conduct regular audits of trading activity.

Execution of Orders and Providing Advice: Firms offering investment advice or executing orders in the crypto space need to adhere to MiCA's guidelines on investor protection and suitability. This involves conducting thorough risk assessments, providing clear information on risks associated with crypto investments and aligning investment recommendations with clients' objectives and risk tolerance.

Staying up to Date with regulatory developments will be essential for CASPs to ensure ongoing compliance with MiCA and regulatory expectations. The Central Bank of Ireland and European Banking Authority expect timely preparatory steps to be taken to prepare to meet the full requirements of the MiCA regulation. The Central Bank has established a cross-sector team to integrate MiCA into their supervisory processes and supervision is likely to be a fast follower following the applicability of all rights and provisions.



MiCA will take effect in Ireland from 30 June 2024.

European Member states had the discretion to shorten the MiCA transition period where

they felt their national regulatory framework was more lenient than the new regulation.

The Department of Finance made the decision to apply this discretion, reducing the transitional period to 12 months. The Central Bank of Ireland will operate as the National Competent Authority, supporting implementation and conducting supervision.

9 June 2023

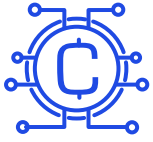
MiCA was published in the Official Journal of the European Union

30 June 2024

MiCA will become applicable for issuers of ARTs and issuers of EMTs

30 December 2024

MiCA will become applicable for issuers of utility tokens and CASPs



How can KPMG help?

KPMG's Risk and Regulatory Consulting Practice is well versed in supporting firms with regulatory compliance and consumer protection. We have a clear understanding of how to prioritise safeguarding consumer interests, with experience guiding firms in meeting MiCA requirements, preparing for regulatory change and strengthening consumer protection measures.

01

KPMG can assist you with a readiness assessment and identify required changes to be implemented. We have extensive experience in providing comprehensive support in licensing and operating requirements to ensure conduct, compliance and regulatory expectations are met.

02

KPMG has tried and tested methodologies to conduct regulatory gap analysis, ensuring gaps and weaknesses are promptly identified. Our systematic approach is comprehensive and ensures clear recommendations that are actionable and sustainable. We can also offer post implementation reviews to support assurance on MiCA regulatory compliance.

03

KPMG can help firms establish a programme of work to interpret and understand the impact of required changes to ensure legal and regulatory compliance. We are well versed in considering, reviewing, and assessing the impact of changes on processes, procedures, technology within banks, financial services and fin tech organisations.

04

KPMG expertise includes evaluating Risk Assessment and Conduct Risk Frameworks for financial products, analysing the effects of regulatory modifications on customer journeys and creating strategies to ensure positive consumer experiences.

05

Drawing on our vast experience in advising clients on consumer-related matters such as product governance, customer assurance and equitable outcomes, KPMG can help crypto-asset service providers to meet expectations on safeguarding consumer and investor interests.

06

KPMG can help firms establish a programme of work to interpret and understand the impact of required changes to ensure legal and regulatory compliance. We are well versed in considering, reviewing, and assessing the impact of changes on processes, procedures, technology within banks, financial services and fin tech organisations.

07

KPMG expertise includes evaluating Risk Assessment and Conduct Risk Frameworks for financial products, analysing the effects of regulatory modifications on customer journeys and creating strategies to ensure positive consumer experiences.



Contact us



Yvonne Kelleher
Managing Director
Risk Consulting
Tel: +353 87 050 4349
e: yvonne.kelleher@kpmg.ie



Matthew Green
Managing Director
Regulatory
Tel: +353 87 050 4377
e: matthew.green@kpmg.ie



Grace Kavanagh
Director
Risk Consulting
Tel: +353 87 744 2582
e: grace.kavanagh@kpmg.ie



Evan O'Leary
Manager
Risk Consulting
Tel: +353 87 050 4461
e: evan.oleary@kpmg.ie



[kpmg.ie](https://www.kpmg.ie)

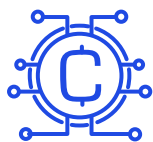
© 2024 KPMG, an Irish partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks of KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

If you've received this communication directly from KPMG, it is because we hold your name and company details for the purpose of keeping you informed on a range of business issues and the services we provide. If you would like us to delete this information from our records and would prefer not to receive any further updates from us please contact unsubscribe@kpmg.ie.

Produced by: KPMG's Creative Services. Publication Date: May 2024. (10390)



Definitions

Crypto Asset	A crypto-asset is a digital or virtual asset secured by cryptography and functioning within a decentralised network, usually a blockchain. These particular assets serve various purposes, including as mediums of exchange, stores of value or units of account. Examples include Bitcoin, Ethereum and other alternative cryptocurrencies.
MiCA	MiCA stands for the Markets in Crypto-Assets Regulation, a regulatory framework proposed by the European Commission to oversee crypto-assets and associated activities within the European Union. MiCA seeks to offer clarity and legal assurance for issuers, service providers and investors engaged in crypto-assets while promoting innovation within the EU's financial sector. Its objective is to establish a comprehensive set of regulations aimed at ensuring consumer protection, market integrity and financial stability in the dynamic crypto-asset market.
E-money tokens (EMTs)	EMTs are a class of digital currency characterised by stable value tied to an official currency and utilising distributed ledger technology. They fall under EU regulations as e-money, requiring a white paper prospectus for issuance and ongoing updates, with both issuers and management bodies held personally liable for the accuracy and completeness of the white paper. Holders are entitled to redemption at par value.
Exchanges for Cryptocurrencies	Exchanges are platforms or market venues where cryptocurrencies are traded between buyers and sellers. These platforms facilitate transactions and provide a centralised or decentralised space for trading. They are essential for enabling liquidity, price discovery and the efficient allocation of resources in financial markets. Exchanges can take different forms, including cryptocurrency exchanges.
Wallet Providers	Wallet Providers are organisations or services that furnish individuals with tools and platforms to securely store, manage and engage with their digital assets, particularly cryptocurrencies. Their main objective is to provide users with a convenient and secure means to store and utilise their digital assets. Wallet providers each have distinct features and security levels and may offer different kinds of wallets, such as software wallets, hardware wallets, web-based wallets and mobile wallets. These providers typically supply software or applications (termed wallets) which empower users to create and oversee their cryptographic keys, allowing them to access and conduct transactions with their cryptocurrency holdings.
CAPs	CAPs are short for Cryptocurrency Asset Providers and play a vital role in facilitating the adoption, trading and management of cryptocurrencies by offering a range of services and platforms to users. They are entities or services engaged in creating, exchanging, distributing or managing cryptocurrency assets. This term encompasses various actors in the cryptocurrency ecosystem, including wallet providers, cryptocurrency exchanges, cryptocurrency custodians and related service providers.
Automated Response Technologies (ARTs)	ARTs are systems or technologies designed to generate responses or perform actions automatically based on predefined rules, algorithms or patterns. In cybersecurity, ARTs can be utilised to promptly detect and address security threats. Overall, ARTs streamline processes, enhance efficiency and increase productivity by automating repetitive tasks and responses. These technologies are applied across different sectors such as cybersecurity, manufacturing and customer service. For example, ARTs may encompass chatbots providing responses to customer inquiries or automated email systems delivering predefined responses to common queries within customer service.
Issuers of utility tokens	Individuals or entities responsible for creating and disseminating digital tokens that grant holders access to specific products, services or functionalities within a blockchain-based ecosystem. Unlike security tokens, which represent ownership in a company or offer dividends, utility tokens serve as digital currency within a particular platform or network. These issuers typically distribute utility tokens through methods such as Initial Coin Offerings (ICOs) or token sales to finance the development and operation of their blockchain projects.