Reply form

**on** **the first Consultation Paper for MiCA implementation**

Responding to this paper

ESMA invites comments on all matters in this paper and in particular on the specific questions summarised in Annex 1 . Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **20 September 2023.**

All contributions should be submitted online at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading ‘*Your input - Consultations’*.

Instructions

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

• Insert your responses to the questions in the Consultation Paper in this reply form.

• Please do not remove tags of the type < ESMA\_QUESTION\_MICA\_0>. Your response to each question has to be framed by the two tags corresponding to the question.

• If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.

• When you have drafted your responses, save the reply form according to the following convention: ESMA\_CP1\_MiCA \_nameofrespondent.

 For example, for a respondent named ABCD, the reply form would be saved with the following name: ESMA\_CP1\_MiCA \_ABCD.

• Upload the Word reply form containing your responses to ESMA’s website (**pdf documents will not be considered except for annexes**). All contributions should be submitted online at *www.esma.europa.eu* under the heading *‘Your input - Consultations’.*

Publication of responses

All contributions received will be published following the close of the consultation unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

Data protection

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading ‘[Data protection](https://www.esma.europa.eu/about-esma/data-protection)’.

Who should read this paper?

All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites crypto-assets issuers, crypto-asset service providers and financial entities dealing with crypto-assets as well as all stakeholders that have an interest in crypto-assets.

# General information about respondent

|  |  |
| --- | --- |
| Name of the company / organisation | x-markets GmbH & Co. KG |
| Activity | Others |
| Are you representing an association? |[ ]
| Country / Region | Germany |

# Introduction

Q0: Please make your introductory comments below, if any:

<ESMA\_QUESTION\_MICA\_0>

x-markets consulting is a specialized consulting firm with more than 20 years of significant functional, technical, and operational expertise mainly in the banking and exchange industry. We have proven our expertise in various projects which are often focused on the implementation of changes in several areas of the capital markets industry, e.g., trading, clearing, settlement, regulation, information security, and digital transformation. Crypto-assets as a new asset class have become strategically relevant for an increasing number of participants, both on the buy and on the sell side of the industry. We therefore thank ESMA for the opportunity to contribute to the discussion of new standards and frameworks. While certain comments below might indicate to primarily reflect the interests of specific stakeholder groups, a well-balanced set of rules and standards considering different perspectives is seen beneficial for the attractiveness and stability of European capital markets for all its stakeholders.

Our introductory comments relate to Crypto Assets Service Providers (CASPs) whose business is custody and administration of crypto-assets on behalf of a third party, which may include provision of a crypto exchange.

We suggest that ESMA’s technical standards for the MiCA implementation should include specific requirements on the important topic of client asset protection for the above mentioned CASPs, i.e., the segregation of clients’ crypto-assets from those assets of the service provider. Following EMIR Articles 39(2) and 39(3) requiring Central Counterparties (CCPs) to offer both ‘individual client segregation’ and ‘omnibus client segregation’, CASPs might also be obliged to offer at least a minimum set of segregation models to its clients.

Related to the segregation of clients’ crypto-assets is the concept of portability and interoperability. Coherent procedures on when and how a client can transfer (port) the own crypto-asset portfolio(s) from one CASP to another support safety and trust among the market participants. In this context, a special focus should lie on scenarios in which the CASP is already in a default situation or is facing a significant risk of a default. However, institutional and retail clients require to have access to their crypto-assets and to be able to transfer those at any time in order to react on stressed market developments, irrespective of (or especially in) a default scenario of their custodian.

For situations in which porting of the crypto-asset portfolios is not possible it might be necessary to liquidate the related portfolios and compensate the customers accordingly. It is suggested to elaborate on setting standards for such liquidation processes. The default management processes of CCPs, which have proven to be main pillars of capital markets safeguards, could serve as blueprints and specific elements like auctions and independent sales could also be established for custodians of crypto-assets on behalf of a third party.

Furthermore, while the technical standards do not specifically mention this, we consider the idea that those CASPs would need to prove the ownership and control of crypto-assets being held in custody a plausible demand in the view of several stakeholders. This evidence would obviously have to be verified by an independent third party, i.e., an auditor. Currently, Proof of Reserves (PoR) concept is a self-regulatory practice introduced by centralized exchanges to demonstrate that they possess adequate reserve of assets. In our view, a high number of CASPs nowadays store their asset data in private, proprietary databases. On-chain PoR for asset managing and holding CASPs can support verify the financial solvency of the CASP to a certain extent. Both, the CASP and the clients would benefit from this trust-gaining transparency. When PoR is combined with client bookkeeping entries, and regular as well as compulsory audits of CASPs, the solvency risk and market disturbance risks would be reduced.

It is our understanding that the most common PoRs algorithms include Merkle tree with user accounts balances data and Zero Knowledge Proofs. The scope of PoR may be extended to include information on the assets involved in lending or liabilities of the company. The audit should be conducted by a reputable auditor in accordance with professionally recognized auditing standards. Once a PoR audit is complete, it could be implemented that the user can find their Merkle leaf and Record ID by logging in to the account and independently verify that the own assets are indeed being held by the CASP. In addition, information on the auditor and further details such as the scope and date of the audit could be made public.

For an additional protection layer relevant CASPs could be required to adequately insure client and company assets. The insurance should offer protection against various risks such as loss, theft or damage to private keys. Insurance for digital assets is seen important for protecting against potential losses and implementing another safeguard for investors. Another option for ESMA to consider could be that clients of CASPs are protected by a European-wide deposit guarantee scheme, based on Directive 2014/49/EU applicable to bank deposits.

Despite the comments above and referring to Article 62 of current MiCA regulation which requires applicants for the CASP licensing to provide description of the current processes of segregation and portability, we suggest verifying whether it could make sense for ESMA’s technical standards to formulate certain exceptions from the segregation of the clients funds and own crypto-assets, e.g., in case of an airdrop or fork. Such unsolicited distribution of crypto-assets and tokens could be sent to the omnibus account, i.e., a wallet address of a pool with assets. We suggest to further analyze if it makes sense that the distribution of such assets to the clients should be provided as it targets generally all wallets with a certain asset or which meet certain requirements. However, the technical standards could determine how CASPs shall manage unsolicited distribution of assets such as airdrops and forks, particularly regarding segregation of client assets.

<ESMA\_QUESTION\_MICA\_0>

# Questions

Q1: Do you think that anything is missing from the draft RTS and ITS on the notification by certain financial entities to provide crypto-asset services referred to in Articles 60(13) and 60(14) of MiCA?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q2: Do you agree with the list of information to be provided with an application for authorisation as a crypto-asset service provider? Please also state the reasons for your answer.:

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q3: Do you agree with ESMA’s proposals on standard forms, templates and procedures for the information to be included in the application for authorisation as a crypto-asset service provider? Please also state the reasons for your answer.

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q4: Do you agree with ESMA’s proposals to specify the requirements, templates and procedures for the handling of client complaints by crypto-asset service providers? Please also state the reasons for your answer.

<ESMA\_QUESTION\_MICA\_0>

ESMA’s proposals for the handling of client complaints by CASPs are well received as generally being considerate and practical. While the intention of the proposal is understood, there might be a few trust gaining additions. However, those additions imply additional operational efforts for the CASPs and therefore should be validated diligently.

CASPs would need to investigate on client complaints in a timely and fair manner. Therefore, it could make sense to, e.g., agree on reasonable standard processing times together with the CASPs which would then serve as timeframe indication for the involved parties during a dispute. In addition, it might be helpful to publish the contact information for an escalation level together with the contact information of the regulatory / supervisory authority which oversees the CASP / under which jurisdiction the CASP falls.

While the policy principle under paragraph 86 of the Complaints Management is seen commendable, we think there might be some challenges in the implementation. For instance, how does a CASP determine that the dedicated resource has the required expertise? Paragraph (b) of Article 11 on Complaints handing under 9.2.3 RTS on authorization of CASPs attempts to solve this problem by requiring that a CASP provides the competent authority with a curriculum vitae. It is questionable if this a sustainable long-term solution for the competent authority.

Paragraph 95 ‘Procedures to ensure consistent complaints-handling’ will certainly help foster investor protection and help generate trust in crypto-asset services and CASPs. Here, we feel that for the benefit of the entire crypto ecosystem, it might serve ESMA well if CASPs periodically share data on the information of the complaint and its subsequent handling with ESMA or the national regulator.

<ESMA\_QUESTION\_MICA\_0>

Q5: Do you think that it is useful to keep the possibility for clients of CASPs to file their complaints by post, in addition to electronic means?

<ESMA\_QUESTION\_MICA\_0>

Yes, it is our opinion that it should be as easy as possible for clients to raise complaints. This includes to file the complaints by post.

<ESMA\_QUESTION\_MICA\_0>

Q6: Do you think that other types of specific circumstances, relationships or affiliations should be covered by Articles 1 and 2 of the draft RTS on the identification, prevention, management and disclosure of conflicts of interest by crypto-asset service providers?

<ESMA\_QUESTION\_MICA\_0>

1. Miner/maximal extractable value (MEV)

Aiming for well-trusted and transparent European capital markets, we support the idea that certain types of MEV activities by the European-domiciled entities should be in scope of the market abuse prohibition policy for CASPs, like the Market Abuse Regulation applied in the traditional financial markets. Particularly, this should involve front running and so-called sandwich-attacks, which result in an unfair arbitrage opportunity, market manipulation and cornering of the market.

Article 80 MiCA prohibits market manipulation and could be extended to ESMA policy taking into account MEV activities. Sandwich-attacks involve front running a trade once it is broadcasted on chain, which affects the price of the trade and the slippage. Moreover, client pending orders should not be used for the market manipulation by CASPs. Such attacks can be tracked on chain and shall be reported under market abuse regulation.

In the recent Policy Recommendation for DeFi Consultation Paper by the IOSCO, MEV takes one of the central parts and is referred to as “the exploitation of mempool data by persons or entities participating in a blockchain’s consensus mechanism (i.e., miners, validators, or other participants) to maximize their profit by choosing and sequencing proposed transactions from the mempool and/or inserting other transactions that are added to a block to be appended to a blockchain“. This practice is considered manipulative and unlawful by IOSCO and it is recommended for regulators to “hold a provider of a DeFi product or service responsible for identifying and, to the extent practicable, managing and mitigating the impact of MEV strategies used by miners/validators on the underlying blockchain on which the provider chooses to operate or offer the product or service”. Again, aiming for well-trusted and transparent European capital markets, it could thus make sense to extend the IOSCO recommended regulation to any European-domiciled entities involved in MEV-based attacks.

2. Insider trading and conflict of interest

Insider trading standards for the employees and operators of the European-domiciled CASPs shall reflect the EU MAR (Article 14): “a person possesses inside information and uses that information by acquiring or disposing of, for its own account or for the account of a third party, directly or indirectly, financial instruments to which that information relates”. The use of inside information by cancelling or amending an order concerning a financial instrument to which the information relates where the order was placed before the person concerned possessed the inside information, shall also be considered to be insider dealing. In relation to auctions of emission allowances or other auctioned products based thereon that are held pursuant to Regulation (EU) No 1031/2010: “the use of inside information shall also comprise submitting, modifying, or withdrawing a bid by a person for its own account or for the account of a third party.” In our opinion, it would make sense to also include non-public information such as the token listings on centralized exchanges, information on upcoming ICOs, IDOs, airdrops, which can affect the prices of the crypto-assets or/and result in unfair trading opportunities.

3. Liquidity lock-up for token issuers (“Rug pull” threat)

Certain CASPs, in particular liquidity providers or crypto-currency token issuers, could be obliged to implement a certain token or liquidity lock-up periods to ensure sufficient liquidity in the market and avoid fraudulent activities commonly known as “rug pulls”.

Such a lock-up period can be coded into the smart contract of the token. If liquidity isn’t locked the owners of the tokens are able to withdraw the full liquidity from the exchange and cash out the whole value. Securities Act Rule 144 in the US could be taken as a reference for this recommendation. To comply with Rule 144, the investor must hold the securities for a certain period of time before it can be sold.<ESMA\_QUESTION\_MICA\_0>

Q7: Do you think that other types of specific prevention or mitigation measures should be highlighted in the minimum requirements of Article 3 of the draft RTS on the identification, prevention, management and disclosure of conflicts of interest by crypto-asset service providers?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q8: Do you agree with the information request laid down in Article 1 and with the granularity envisaged for the information to be provided by proposed acquirers that are trusts, AIF or UCITS management companies or sovereign wealth funds?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q9: Do you agree with the proportionate approach to the request of information to be submitted by proposed indirect acquirers of qualifying holdings based on whether they are identified via the control or the multiplication criterion?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q10: Do you consider the list of information under Article 8 complete and comprehensive to assess the financing of the acquisition, in particular as regards funding originated in the crypto ecosystem?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q11: Do you agree with the identified cases where reduced information requirements apply and with the related requirements and safeguards?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q12: In which EU jurisdiction(s) do you plan to be authorised to provide CASP services? In which EU jurisdiction(s) do you plan to provide CASP services under cross-border provision of crypto-asset services as specified in Article 65 of Regulation (EU) 2023/1114?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q13: What crypto asset services as listed in point 16 of Article 3(1) of Regulation (EU) 2023/1114 do you plan to offer (e.g. reception/transmission of orders; execution of orders on behalf of clients; operation of a trading platform etc.)? In addition, please provide some high-level explanation of the business model, including, what type of trading systems do you plan to use.

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q14: If you are planning to operate a trading platform:

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(a) How many white papers do you estimate to publish on you platform?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(b) What turnover, in terms of crypto-assets trading volume, do you expect to attract on your platform according to your business forecasts for the upcoming years?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(c) Do you plan to undertake transactions on the basis of an on-chain ledger or an off-chain one?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

 i. In case of the former, which type of DLT are you planning to use (e.g. Ethereum, Corda, Stellar etc.)? Do you plan to store transaction data on-chain or off-chain or a mix of the two?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

 ii. If the latter, how would you link on-chain and off-chain transaction data?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q15: If you are planning to execute/place orders on behalf of clients:

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(a) How many white papers do you estimate to offer to your clients for execution/order placement?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(b) What is the expected turnover (i.e. revenues) according to your business forecasts for the upcoming years?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(c) Do you plan to undertake transactions on the basis of an on-chain ledger or an off-chain one?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

 i. In case of the former, is transaction data stored on-chain or off-chain or a mixed of the two?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

 ii: If the latter, how do you link on-chain and off-chain transaction data?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

Q16: If you are planning to receive and transmit orders:

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(a) How many white papers do you estimate to offer to your clients for order transmission?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(b) What is the expected turnover (i.e. revenues) according to your business forecasts for the upcoming years?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(c) Which are the main platforms/brokers you are intending to transmit orders to?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(d) In which jurisdictions are these platforms/brokers based?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>

(e) How do you plan to keep track of the transmitted orders?

<ESMA\_QUESTION\_MICA\_0>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MICA\_0>