

Response to the European Commission's targeted consultation on the review of MiCA

VASPnet's written answers, by question

On 30 September 2026, VASPnet submitted a response to the European Commission's targeted consultation on the review of Regulation (EU) 2023/1114 (MiCA). This document reproduces VASPnet's 14 written answers under the Commission's question numbers. Questions answered only by selecting rating options are not included. Question text is abridged. The full wording is in the [Commission's consultation questionnaire](#).

The accompanying article sets out the findings and the implications for financial institutions: [VASPnet's response to the European Commission's MiCA review](#).

Summary of responses

#	Question (abridged)	Response summary
4	Remaining concerns after initial MiCA implementation	Regulatory status is often not binary. Enforcement depends on reliable entity-level identification and consistent publication of regulatory data.
28	Importance of EU access to global stablecoins via EU issuers and CASPs	Highly important, as EU-authorised entities are identifiable access points. Entity status is one part of the risk picture. Wider group data is also needed.
29	Risks of a multi-issuance model for global stablecoins	Multi-issuer arrangements add supervisory complexity and arbitrage risk. Transparency on legal and regulatory structure is needed.
40	Merit of an equivalence regime for global stablecoins	Supports equivalence based on comparable outcomes. Jurisdiction-level equivalence should not replace entity-level assessment.
41	How far reliance on a third-country regime should go	Reliance should rest on minimum transparency expectations, supervisory cooperation and current entity-level data.
45	Adequacy of the Article 3(16) list of crypto-asset services	Provider terminology does not map neatly to MiCA categories. Consistent publication of authorised activities would add clarity.
48.1	Promotion by non-EU providers and available enforcement tools	Providers continue to serve EU customers, some under NCA forbearance. Calls for supervision and enforcement, not guidance alone, and a payments reporting regime.
51.1	Oversight of entities offering other services alongside crypto-asset services	Entity-level authorisation does not show the wider group. Supports cooperation between competent authorities and consistent group data.
52	Regular reporting by CASPs	Supports reporting built on standardised core data and recognised identifiers.
56.1	EU liquidity or full access to global liquidity	Access to global liquidity matters. Assess the specific legal entity, with proportionate due diligence.
57	Proportionality of MiCA Level 1 rules for CASPs	Scope to simplify through standardised, reusable authorisation information across competent authorities.
61	Criteria for assessing the decentralisation of a DeFi application	Multi-factor assessment. Control by identifiable persons carries more weight than any single technical feature.
62.1	Risks from fully decentralised DeFi applications	Distinguish legal-entity due diligence from protocol-level risk assessment. Where identifiable persons exercise control, CASPs should identify them.
86	Other relevant issues	Recommends interoperability between the MiCA register and regulatory information from other authorities, including on group entities.

Part 1. Scope and definitions (Title II crypto-assets)

4) Based on initial implementation experience under MiCA, please assess the extent to which the following issues remain a concern. Please explain your ratings, focusing on the issues you deem most significant.

MiCA has materially improved regulatory consistency within the EU, but risks of regulatory arbitrage and cross-border enforcement gaps remain, particularly where crypto-asset service providers operate through complex international group structures or continue servicing EU customers from third countries, even where they have an entity incorporated in the Union and CASP licensed.

In practice, regulatory status is often not binary. A provider may be authorised through a local entity in one jurisdiction, registered under a transitional or legacy regime in another, expressly prohibited in a third, and have no identifiable regulatory basis elsewhere. This creates challenges for both supervisors and obliged entities seeking to determine whether a specific legal entity is permitted to provide a particular crypto-asset service, and where that service is being provided from.

Effective enforcement therefore depends on reliable identification of the entities operating within the market. Greater consistency in the publication of regulatory data; including legal entity names, trading names, group relationships, permitted activities, licence status, competent authority and effective dates would improve cross-border supervisory coordination and support regulated firms in meeting counterparty due diligence obligations.

Part 2. Asset-referenced tokens and e-money tokens (Titles III and IV)

28) How important is it for EU users to be able to access global stablecoins via EU-based and licenced issuers and CASPs?

Access to global stablecoins through EU-authorised issuers and crypto-asset service providers provides identifiable, regulated access points through which regulatory, compliance and consumer protection obligations can be applied. As such, it is highly important for EU users.

However, the regulatory status of the EU-based entity represents only one part of the overall risk picture. Global stablecoin arrangements frequently involve multiple legal entities, service providers and regulatory relationships across jurisdictions. An issuer, distributor, exchange, custodian or other participant may therefore be subject to different regulatory regimes, permissions and supervisory expectations depending on where it operates.

For regulated firms conducting counterparty due diligence, it is important to understand not only whether an EU entity is authorised, but also the wider regulatory footprint of the relevant issuer or service-provider group, including the legal entities involved, their permitted activities, competent authorities and status in other jurisdictions.

Facilitating access through EU-authorised entities can provide an important regulatory anchor, but should be complemented by reliable and transparent information concerning the wider group and cross-border structure. This supports effective due diligence, supervisory cooperation and risk assessment without assuming that authorisation of one entity necessarily determines the regulatory standing of the wider global arrangement.

29) How significant are the risks associated with a multi-issuance model of global stablecoins for the EU financial system?

Multi-issuer global stablecoin arrangements create additional regulatory and supervisory complexity, particularly where different entities within the same arrangement are subject to different regulatory regimes, permissions and supervisory authorities.

Legal entities within the same stablecoin ecosystem may have materially different regulatory statuses across jurisdictions. This can make it difficult for regulated firms, supervisors and counterparties to determine which entity is responsible for a particular activity and which regulatory protections apply.

Regulatory arbitrage where issuance, distribution or other material functions are allocated to entities in jurisdictions with differing regulatory requirements is possible. As such, greater transparency around the legal and regulatory structure of multi-issuer arrangements would be valuable.

40) Do you see merit in introducing an equivalence regime for global stablecoins in the EU? Please provide reasons, including any perceived advantages or disadvantages of equivalence regimes.

An equivalence framework for third-country stablecoin regimes could support cross-border interoperability and reduce unnecessary duplication, provided that equivalence is based on comparable regulatory outcomes rather than identical legal structures.

However, jurisdiction-level equivalence should not be treated as a proxy for the regulatory standing of individual entities. For regulated firms conducting counterparty/correspondent due diligence, it remains important to identify the specific legal entity involved, the activities it is authorised to perform, its

competent authority and its current regulatory status. At this time, only a small number of jurisdictions have implemented comprehensive stablecoin regimes.

Any equivalence framework would therefore benefit from reliable, current and comparable regulatory reference data at entity level. This would help supervisors and market participants determine whether a particular entity falls within an equivalent regime and whether its specific activities are appropriately authorised.

41) How far should a possible equivalence regime go in terms of relying on the third-country regime? What rights or benefits should EU issuers and issuers from an equivalent jurisdiction receive?

Jurisdiction-level assessments on equivalence alone may not provide sufficient certainty. Individual issuers and service providers within the same jurisdiction may be subject to different licensing categories, permissions, restrictions, transitional arrangements or enforcement outcomes.

Any reliance framework would benefit from clear minimum expectations around regulatory transparency, including publication of current information on legal entities, regulatory status, permitted activities, competent authorities and effective dates. Comparable and machine-readable regulatory information would also improve consistency and reduce the risk of firms interpreting foreign regulatory statuses differently.

Supervisory cooperation and information-sharing arrangements are also important, particularly where a global stablecoin structure spans multiple jurisdictions.

Accordingly, reliance on third-country regimes can support international interoperability, but should be underpinned by transparent, current regulatory information rather than jurisdiction-level assumptions alone.

Part 3. Crypto-asset service providers (Titles V and VI)

45) Is the list of crypto-asset services in Article 3(16) of MiCA adequate to effectively cover crypto-asset markets and provide sufficient legal clarity for businesses?

From a regulatory reference-data perspective, service providers do not always describe their activities using terminology that maps neatly to the categories set out in MiCA. Trading names, websites and regulatory registers may use different descriptions for substantively similar activities, while individual firms may undertake several functions through different legal entities within the same group.

This can create difficulties for regulated firms seeking to determine not simply whether a provider is authorised, but precisely which legal entity is authorised to perform which activity. A concern is that a regulatory halo effect may apply, whereby a firm makes claims to be regulated, without clarifying what activities it is authorised to undertake.

Greater consistency in how authorised activities are described and published by competent authorities would therefore improve legal and operational clarity. In particular, MiCA service categories should, where possible, be reflected consistently in regulatory registers and made available in structured form at legal-entity level.

48.1) How do non-EU authorised providers promote their services in the EU? What tools would supervisors or enforcement authorities have, or should they have, to

stop non-authorised service providers from offering their services in the EU or to EU customers?

There are several service providers - in third countries and in the EU - that continue to offer their services in the EU. Many of them are known to VASPnet. While guidance on reverse solicitation under MiCA (ESMA35-1872330276-2030) was found to be helpful to distinguish between direct and reverse solicitation, and specifically the narrow scope to which reverse solicitation may be applied, the continued availability of services from non-EU crypto-asset service providers presents an important supervisory and enforcement challenge.

Several service providers in the EU that are progressing their application to operate under MiCA have been informally advised by their NCA to continue offering services, while the NCA applies forbearance to such services. Others have been informed that doing so would be in contravention of the terms of the transitional period, resulting in them halting all services, ceasing their operations and transitioning their customers to MiCA licensed CASPs.

A consistent and accessible view of authorised, non-authorised and otherwise restricted providers would also support counterparty due diligence and reduce the risk of firms relying on assumptions based solely on brand recognition or authorisation held by another entity within the same group.

VASPnet today helps banks and other FIs to identify fiat-crypto ramping events by identify crypto related payments. A valuable instrument for supervisors and enforcement authorities would be a reporting regime applicable to payment institutions, EMLs and credit institutions that would require the listing of CASP payment counterparties, the regulatory status of such CASPs and their respective cumulative payment value.

The significant uplift between the majority of crypto-asset regimes and MiCA, together with the narrow scope of reverse solicitation requires not just guidance but supervision and enforcement to ensure that a level playing field exists for EU CASPs.

51.1) Which enhanced oversight and coordination mechanisms may be appropriate for entities that offer other unregulated or regulated services alongside crypto-asset services?

Multi-function crypto-asset groups can create supervisory challenges where activities are distributed across multiple legal entities, jurisdictions and regulatory regimes.

An entity-level authorisation provides important information, but may not provide a complete view of the wider group through which services are delivered. A regulated CASP may form part of a broader structure containing other regulated entities, unregulated operating companies, technology providers, custodians or entities authorised under different financial-services regimes.

For supervisors and regulated counterparties, understanding these relationships can be important when assessing operational dependencies, conflicts of interest, concentration risk and the regulatory basis on which different activities are performed.

Enhanced cooperation between competent authorities may therefore be appropriate for larger or more complex groups, particularly where material activities span several Member States or third countries. Any group-level reporting or supervisory framework should, however, remain proportionate to the nature, scale and complexity of the group.

Greater consistency in the publication of group relationships, legal entities, regulatory status and permitted activities would also improve supervisory visibility. This would help ensure that authorisation of one entity is not incorrectly assumed to extend to other entities operating under the same brand or within the same corporate group.

52) Should CASPs report regularly on their activities?

Please specify what kind of reporting would be useful and how often.

Regular reporting by crypto-asset service providers can improve supervisory visibility, particularly where it captures material counterparty exposures and dependencies. However, the usefulness of such reporting depends heavily on the quality and consistency of the underlying counterparty data.

For crypto-asset markets, identifying the relevant counterparty can be challenging where services are provided through trading names, multiple legal entities or international group structures. A meaningful assessment of counterparty risk therefore requires firms to identify the specific legal entity involved, its regulatory status, permitted activities, competent authority and relationship to the wider group.

Any reporting framework should seek to standardise these core data points and use recognised identifiers wherever possible. This would improve comparability across firms and reduce the risk that the same counterparty is reported differently by different CASPs.

This would help ensure that counterparty reporting reflects the actual legal and regulatory relationships within the market rather than relying on brand-level or self-declared information.

56.1) What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

Access to global trading venues and liquidity pools can be important for EU CASPs, particularly where liquidity is concentrated across international markets. However, such access also creates additional counterparty and regulatory-perimeter considerations.

The relevant risk assessment should focus on the specific legal entity providing the service or liquidity rather than solely on the trading venue,

brand or corporate group. Global crypto businesses frequently operate through multiple entities subject to different regulatory regimes, permissions and supervisory authorities. An entity may be appropriately authorised in one jurisdiction while another entity within the same group may have a materially different regulatory status.

EU firms accessing non-EU liquidity should therefore be able to identify the legal counterparties involved, understand the regulatory basis on which they provide the relevant services, quality of supervision, and assess their wider group relationships and jurisdictional footprint.

Greater transparency and consistency in regulatory reference data would support this process, particularly where information on non-EU providers is fragmented across multiple regulatory registers.

Accordingly, preserving access to global liquidity should be accompanied by proportionate counterparty due diligence and clear entity-level regulatory information, rather than assumptions based solely on the reputation or regulatory standing of a global trading brand.

57) Do the MiCA level 1 provisions for CASPs lay down proportionate and simple-to-apply rules, taking into account size, scope of activity and risk profile? Please suggest how rules could be made simpler and more proportionate.

There remains scope to improve proportionality and operational simplicity, particularly in relation to authorisation information and ongoing regulatory disclosures.

From a regulatory reference-data perspective, one source of friction is the inconsistent way in which information on authorised firms is published across competent authorities. Differences in terminology, data fields, update frequency and identifiers can make it difficult for market participants to

determine an entity's current status and the precise activities it is permitted to perform.

Greater standardisation of core regulatory information would improve usability without reducing supervisory standards. This could include consistent publication of legal entity names, trading names, authorisation status, permitted services, competent authority, relevant dates and recognised identifiers where available.

Where possible, information already collected through the authorisation process should be capable of being reused across supervisory, reporting and compliance processes rather than recreated in different formats.

This would reduce unnecessary administrative burden while improving transparency, comparability and the ability of regulated firms to conduct effective counterparty due diligence.

Part 4. Topics beyond the initial scope of MiCA

61) Which criteria should be used to assess the degree of decentralisation of a DeFi application?

Particular weight should be given to whether an identifiable person or group can control, suspend, upgrade or materially alter key protocol functionality, including through administrator keys, governance rights or other privileged access. Significant concentration of governance power may also be relevant where it enables effective control over the operation of the protocol.

The existence of an identifiable entity actively providing access to, operating or marketing a protocol may also be relevant, although marketing alone should not necessarily determine whether a protocol is decentralised.

Other factors, such as whether code is open source or whether assets are held in custody, may provide useful contextual indicators but should not, in isolation, determine regulatory classification. Should the DeFi arrangement have been governed in a centralised manner in the past should also be considered, given that legacy control often continues even under a decentralised governance model. Gaps in governance and control that are not presented in formal policies may present 'off-chain' governance, which can include delegated voting rights.

A principles-based, multi-factor assessment would therefore be preferable to reliance on any single technical characteristic. The central question should be whether identifiable persons retain sufficient control or operational responsibility such that the activity is substantively intermediated notwithstanding the use of decentralised technology.

62.1) How should MiCA account for risks from fully decentralised DeFi applications?

Unlike conventional counterparties, a fully decentralised protocol may not have a legal entity, regulated operator or identifiable controlling person against which traditional counterparty due diligence can be performed. The assessment may instead need to consider factors such as protocol governance, identifiable controllers or developers, administrator or upgrade rights, smart-contract risk, custody arrangements, sanctions exposure and material dependencies on third-party service providers.

Requirements should therefore distinguish between legal-entity due diligence and technical or protocol-level risk assessment. CASPs should not be expected to establish regulatory status where no identifiable regulated counterparty exists. However, it is not always evident when a firm is DeFi in name, or in practice. As such, it is valuable for a trusted third party to share such information or the obliged entity determines it to be the case given appropriate subject matter expertise. Failure to do this, while welcoming engagement with DeFi arrangements may result in an exploitable risk nexus.

Where identifiable persons or entities do exercise material control, however, CASPs should seek to understand their identity, role and, where applicable, regulatory status.

Any framework should remain risk-based and proportionate, recognising that the extent of due diligence reasonably available will vary considerably depending on the architecture and degree of decentralisation of the protocol.

86) Interested parties that wish to bring other relevant issues, not raised in this consultation, to the Commission's attention may communicate them here.

One additional issue that merits consideration is how information contained in the MiCA register can be used effectively alongside regulatory information concerning crypto-asset service providers outside the MiCA framework.

The ESMA register established under Article 109 provides an important source of information on MiCA-authorised CASPs. However, regulated firms conducting counterparty due diligence frequently need to understand a broader regulatory footprint, particularly where a provider operates through multiple legal entities, trading names and jurisdictions. Articles 59, 60, 63 and 109 may benefit from the inclusion of language that registers, and makes available information on third country firms - and entities of EU CASPs - that are registered and offering services to EU users.

For example, an EU-authorised CASP may form part of an international group containing entities subject to different regulatory regimes, while other providers accessible to EU counterparties may neither appear on the MiCA register nor on the non-exhaustive register of non-compliant entities established under Article 110. Non-compliant entity registers are also inconsistently presented across member states.

Greater interoperability between MiCA regulatory information and equivalent information published by other EU and third-country authorities would therefore support effective counterparty due diligence and regulatory perimeter monitoring. Consistent identifiers, activity classifications and machine-readable information would make it easier to determine which legal entity is providing a service, under which regulatory permission and as part of which wider group.

This would complement, rather than duplicate, the existing MiCA register while improving its usefulness within an increasingly global crypto-asset market.

About VASPnet

VASPnet is the world's assured source of regulatory data on virtual asset service providers (VASPs). Our VASPdata and VASPindex products give public and private sector entities the information they need to make well-informed, risk-based decisions on the VASPs they do business with. VASPnet is a division of CRB Monitor, a global data provider focused on newly regulated markets.

To find out more, visit vaspnet.com and follow us on [LinkedIn](#).

Contact us at info@vaspnet.com

Author

Neil Samtani

30 September 2026

Copyright © 2026 Enhanced Compliance Solutions, Inc. All rights reserved.

VASPnet® is a registered trademark of Enhanced Compliance Solutions, Inc.
VASPdata is a trademark of Enhanced Compliance Solutions, Inc.

This document is for informational purposes only and is not legal or financial advice. Reader reliance on this information is at their own risk.