EUROPEAN
COMMISSION

Brussels, 31.10.2024
C(2024) 7523 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 31.10.2024

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA) was published in the Official Journal of the European Union on 9 June 2023 and entered into force on 29 June 2023. MiCA starts applying on 30 June 2024 as regards Titles III and IV on issuers of asset-referenced tokens (ARTs) and e-money tokens (EMTs) respectively, and is fully applicable as of 30 December 2024.

MiCA regulates issuers of crypto-assets that are not already covered by other financial services acts as well as providers of services in relation to such crypto-assets (crypto-asset service providers). Its objective is to promote safe and sustainable innovation while addressing the risks to consumers, market integrity, financial stability as well as the risks to monetary policy transmission and monetary sovereignty arising from this new class of assets.

Article 68(7) of MiCA requires crypto-asset service providers to take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services. To that end, crypto-asset service providers are required to employ appropriate and proportionate resources and procedures, including resilient and secure ICT systems as required by Regulation (EU) 2022/2554. Furthermore, under that article, crypto-asset service providers must establish a business continuity policy, which should include ICT business continuity plans as well as ICT response and recovery plans set up pursuant to Articles 11 and 12 of Regulation (EU) 2022/2554 that aim to ensure, in the case of an interruption to their ICT systems and procedures, the preservation of essential data and functions and the maintenance of crypto-asset services or, where that is not possible, the timely recovery of such data and functions and the timely resumption of crypto-asset services. Under Article 68(10) of MiCA, ESMA is mandated to develop draft technical standards that specify measures for ensuring continuity and regularity in the performance of crypto-asset services.

Article 68(10) of MiCA empowers the Commission to supplement the regulation by adopting the regulatory technical standards drafted by ESMA.

This delegated act is to be adopted in accordance with Article 68(10) of MiCA and Article 290 of the Treaty on the Functioning of the European Union.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

ESMA prepared the draft regulatory technical standards and conducted an open public consultation between 5 October 2023 and 14 December 2023.[1] Among the 141 stakeholders which responded to the consultation which covered also other technical standards, there was an average of 20 responses across 7 questions relating to the consulted draft technical standards. Responses came from a range of stakeholders, including traditional exchanges, crypto firms, trade associations, and asset managers. Below is an overview of the feedback to the salient questions discussed in the consultation.

On introducing the concept of permissionless distributed ledgers, most respondents supported a specific definition for such networks, but noted it should be made clear in the technical standards that CASPs would be required to have 'effective control' of the DLT to ultimately

[1] https://www.esma.europa.eu/sites/default/files/2024-03/ESMA18-72330276-1634_Final_Report_on_certain_technical_standards_under_MiCA_First_Package.pdf

be liable for any service disruptions or other operational incidents caused by the DLT. Several respondents argued that introducing a distinction between the two types of distributed ledgers in the draft standards would create more confusion for the market. They preferred to maintain consistency with Article 75(8) of MiCA, which introduces the concept of control without going into the technical aspects of each type of DLT. In order to ensure clarity and convergence, the final standards include a definition of permissionless distributed ledgers.

On the question whether the technical standards should specify that CASPs are required to establish a specific business continuity management function, several respondents indicated that mandating a business continuity management function would be too prescriptive relative to the mandate. Nonetheless, a high number of respondents supported the notion that there should at least be resources dedicated to business continuity within a CASP. The final standards therefore do not include a requirement for a specific business continuity management function.

Furthermore, the consulted version of the draft technical standards comprised a requirement for an independent assessor (either a separate function within the CASP's organisation or a third-party provider) to review the management body's assessment of the implementation of the CASP's business continuity measures (policy, plans and procedures). This provision was subsequently removed by ESMA, partly because most respondents objected to it as being outside the mandate and disproportionate.

In Article 6 of the draft technical standards, ESMA proposes a general principle on risk considerations, which among others, calls for CASPs to take into consideration the degree to which the availability of their services would depend on DLTs they do not control for the purposes of their business continuity plans. Part of this principle is a self-assessment to be completed by the CASP, which is aimed at ensuring that they take into due consideration the risk factors that may cause or prolong interruptions in the availability of their services and at providing supervisors with a tool to assess if CASPs are implementing business continuity procedures commensurate with the risks they pose. The general principle on risk considerations in Article 6 of the draft technical standards received broad support from respondents. Some comments suggested to clarify explicitly that the self-assessment obligation stems from Article 68(8) of MiCA. On the self-assessment, most respondents supported the proposal and the criteria listed in the Annex (with several caveats and requests for extensions), with one respondent suggesting to extend the minimum timeframe for the self-assessment from at least annually to bi-annually to ease the burden on CASPs.

In addition to the public consultation, ESMA asked for the advice of the Securities and Markets Stakeholder Group (SMSG), which was delivered on 13 December 2023. In particular, the SMSG noted the importance of business continuity requirements in ensuring orderly markets. Furthermore, it explicitly supported the approach to proportionality for business continuity proposed in Article 6 of the draft technical standards, including the proposed self-assessment, as it allows each entity to calibrate business continuity measures on their own needs. The SMSG also noted it did not see a need to require the establishment of a dedicated business continuity function to oversee the obligations in the technical standards; rather this should be merely an option left to the decision of the CASP's management body, also taking into account the need to maintain proportionality of regulatory burden.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Article 1 comprises definitions.

Article 2 provides for requirements regarding the organisational aspects of the business continuity arrangements to be maintained by CASPs.

Article 3 lays down the requirements applicable to the business continuity policy to be established by CASPs, including its essential elements.

Article 4 requires CASPs to establish business continuity plans to implement the business continuity policy and specifies their minimum content.

Article 5 specifies the requirements for the periodic testing of business continuity plans to be undertaken by CASPs.

Article 6 requires CASPs to take into account the increased complexity and risk when developing their business continuity policy and, in this context, to carry out a self-assessment of the scope, nature and range of their services.

Article 7 provides for the date of entry into force of the regulation and its applicability in Member States.

COMMISSION DELEGATED REGULATION (EU) …/...

of 31.10.2024

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulation (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[2], and in particular Article 68(10), third subparagraph, thereof,

Whereas:

(1) Articles 11 and 12 of Regulation (EU) 2022/2554 of the European Parliament and of the Council[3] provide for requirements relating to response and recovery, backup policies and procedures, restoration and recovery procedures and methods concerning the ICT systems of financial entities, including crypto-asset services providers. Commission Delegated Regulation (EU) 2024/1774[4] further specifies components of the ICT business continuity policy, the testing of ICT business continuity plans, the components of the ICT response and recovery plans of financial entities, including crypto-asset service providers. This Regulation complements those provisions of Regulation (EU) 2022/2554 and of Commission Delegated Regulation (EU) 2024/1774 with respect to continuity and regularity in the performance of the crypto-asset services.

(2) In providing their services, crypto-asset service providers may use a distributed ledger over which they have no control, including a permissionless distributed ledger. In that case, they may not be capable of ensuring the regularity and continuity of their services when disruptions are caused by problems that are inherent to the operation of

[2] OJ L 150, 9.6.2023, p.40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

[3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[4] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (OJ L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj).

such distributed ledgers. To mitigate market volatility that may have an adverse impact on clients affected by such disruptions, crypto-asset service providers should include in their business continuity policy measures for timely communication with clients and other external stakeholders. Such communication should include essential and timely information for clients on such disruptions, including ongoing status updates, until the disruption is resolved and services are resumed. Where information on the status of the permissionless distributed ledger responsible for a service disruption is not readily available to the crypto-asset service provider, that crypto-asset service provider should communicate updates to clients and other stakeholders, including competent authorities, on a best effort basis to ensure that clients and stakeholders have as comprehensive information as possible on such disruptions.

(3) To avoid disproportionate administrative burden for small and medium-enterprises and start-ups, crypto-asset service providers should consider in their business continuity policy the scale, nature, and range of the services they provide. That means that crypto-asset service providers should determine their specific business continuity requirements on the basis of a robust self-assessment, based on a number of criteria that would enable them to implement a business continuity policy that is commensurate with the market impact of their services. The self-assessment should also take into account other circumstances beyond those listed in the Annex that may have an impact on the crypto-asset service provider.

(4) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority.

(5) The European Securities and Markets Authority has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[5],

HAS ADOPTED THIS REGULATION:

Article 1
Definitions

For the purposes of this Regulation, the following definitions shall apply:

(a) ‘critical or important function’ means a critical or important function as defined in Article 3, point (22), of Regulation (EU) 2022/2554 of the European Parliament and of the Council;

(b) ‘permissionless distributed ledger’ means a specific type of distributed ledger in which no entity controls the distributed ledger and DLT network nodes can be set up by any person complying with the technical requirements and the protocols of that distributed ledger.

[5] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

Article 2
Business continuity organisational arrangements

1. The business continuity policy referred to in Article 68(7) shall be comprised of plans, procedures and measures.

2. The management body of crypto-asset service providers, in the exercise of its functions referred to in Article 68(6) of Regulation (EU) 2023/1114, shall establish and endorse the plans, procedures, and measures that comprise the business continuity policy. The crypto-asset service provider's management body shall be responsible for the implementation of the business continuity policy, and for reviewing its effectiveness at least on an annual basis.

3. Crypto-asset service providers shall ensure that any modifications to the business continuity policy are transmitted to all relevant internal staff through effective communication channels.

Article 3
Business continuity policy

1. The business continuity policy referred to in Article 68(7) of Regulation (EU) 2023/1114 shall ensure that crypto-asset service providers properly address disruptive incidents or performance issues relating to the systems critical to the operation of their business functions and it shall be laid down in a durable medium.

2. Crypto-asset service providers shall include in the business continuity policy all of the following:

   (a) a specification of the scope of the business continuity policy, including its limitations and exclusions, to be covered by the business continuity plans, procedures, and measures;

   (b) a description of the criteria to activate the business continuity plans, including escalation procedures up to the level of the management body;

   (c) provisions on the governance and organisation of the crypto-asset service provider, including, the roles and responsibilities of the staff, ensuring that sufficient resources are available for the effective implementation of the policy;

   (d) provisions that ensure consistency between the business continuity plans and the ICT-business continuity plans, and ICT response and recovery plans referred to in Articles 24 and 26 of Commission Delegated Regulation (EU) 2024/1774.

Article 4
Business continuity plans

1. When implementing the business continuity policy referred to in Article 68(7) of Regulation (EU) 2023/1114, crypto-asset service providers shall establish business continuity plans. The business continuity plans shall set out the procedures necessary to protect and, where necessary, re-establish:

   (a) the confidentiality, integrity, and availability of client data;

   (b) the availability of the business functions, supporting processes and information assets of the crypto-asset service providers.

2. The business continuity plans shall contain the following:

(a) a range of possible adverse scenarios relating to the operation of critical or important functions, including the unavailability of business functions, staff, workspace, external suppliers, data centres, or loss or alteration of critical data and documents;

(b) the procedures and policies to be followed in case of a disruptive incident, including:

(i) the measures that are necessary to recover critical or important functions;

(ii) the deadlines by which those critical or important functions are to be recovered;

(iii) recovery point objectives;

(iv) the maximum time to resume services;

(c) the procedures and policies for relocating the business functions used to provide crypto-asset services to a back-up site;

(d) back-up of critical business data, including up-to-date information of the necessary contacts to ensure communication inside the crypto-asset service provider, between the crypto-asset service provider and its clients;

(e) procedures for timely communications with clients and other external stakeholders, including competent authorities.

3. In the event of a disruption involving a permissionless distributed ledger used by the crypto asset service provider in the provision of its services, the communications referred to in paragraph 2, point (e) shall include the following information:

(a) when the services are expected to be resumed;

(b) the reasons and the impact of the disruptive incident;

(c) any risks concerning clients' funds and crypto-assets held on their behalf;

(d) measures that the crypto-asset service intends to take in response to the disruption of a permissionless distributed ledger.

Where that information is not readily available to the crypto-asset service provider, the crypto-asset service provider shall communicate updates as regards the information in the first subparagraph to clients and stakeholders, including competent authorities, on a best effort basis.

4. The business continuity plans shall contain procedures to address any disruptions of outsourced critical or important functions, including where those critical or important functions become unavailable.

Article 5
Periodic testing of the business continuity plans

1. Crypto-asset service providers shall test the operation of the business continuity plans referred to in Article 4 on the basis of realistic scenarios. Such testing shall verify the capability of the crypto-asset service provider to recover from disruptive incidents and to resume services in accordance with Article 4(2), point (b).

2. Crypto-asset service providers shall test the business continuity plans annually taking into account:

   (a) the results of the tests referred to in paragraph 1;

   (b) the most recent threat intelligence;

   (c) lessons derived from previous events;

   (d) where relevant, any changes in the recovery objectives, including recovery time objectives and recovery point objectives as referred to in Article 4(2) point (b);

   (e) changes in the business functions.

3. Crypto-asset service providers shall document the results of the testing activity in writing, and submit them to their management body and to the operating units involved in the business continuity plans.

4. Crypto-asset service providers shall ensure that the testing of the business continuity plans does not interfere with normal conduct of their services.

Article 6
Complexity and risk considerations

1. When establishing the business continuity policy, including the plans, procedures and measures, crypto-asset service providers shall take into account elements of increased complexity or risk, including:

   (a) the type and range of crypto-asset services offered;

   (b) the extent to which the services of the crypto-asset service provider rely on permissionless distributed ledger;

   (c) the potential impact of any disruptions on the continuity of the crypto-asset service provider's activities and availability of its services.

2. For the purposes of paragraph 1, crypto-asset service providers shall conduct a self-assessment of the scale, the nature, and range of their services annually. Crypto-asset service providers shall base that self-assessment on the criteria set out in the Annex and any other criteria that the crypto-asset service provider considers relevant.

Article 7
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 31.10.2024

For the Commission
The President
Ursula VON DER LEYEN