

# Final Report

Draft Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – second package

## Table of Contents

1	Executive Summary .....	5
2	Sustainability indicators in relation to climate and other environment-related adverse impacts.....	6
2.1	Background and legal basis .....	6
2.2	Assessment.....	9
3	Measures to ensure continuity and regularity in the performance of crypto-asset services .....	18
3.1	Background and legal basis .....	18
3.2	Assessment.....	18
4	Pre-and-post-trade transparency.....	29
4.1	Background and legal basis .....	29
4.2	Assessment.....	30
5	Record keeping obligations for CASPs.....	42
5.1	Background and legal basis .....	42
5.2	Assessment.....	43
6	Machine readability of white papers and white papers register .....	61
6.1	Background and legal basis .....	61
6.2	Assessment.....	62
7	Technical means for appropriate public disclosure of inside information.....	67
7.1	Background and legal basis .....	67
7.2	Assessment.....	68
8	Annexes .....	81
8.1	Annex I: Cost-benefit analyses.....	81
8.2	Annex II: Advice of the Securities and Markets Stakeholder Group .....	126
8.3	Annex III: Feedback on the Consultation Paper (question-by-question).....	136
8.4	Annex IV: Draft RTS pursuant to Articles 6(12), 19(11), 51(15) & 66(6) of MiCA 178	
8.5	Annex V: Draft RTS pursuant to Article 68(10)(a) of MiCA .....	197

8.6	Annex VI: Draft RTS pursuant to Article 76(16)(a) of MiCA .....	206
8.7	Annex VII: Draft RTS pursuant to Article 68(10)(b) of MiCA .....	226
8.8	Annex VIII: Draft RTS pursuant to Article 76(16)(b) of MiCA .....	276
8.9	Annex IX: Draft ITS pursuant to Articles 6, 19 & 51 of MiCA.....	311
8.10	Annex X: Draft RTS pursuant to Article 109(8) of MiCA.....	401
8.11	Annex XI: Draft ITS pursuant to Article 88(4) of MiCA .....	413

## List of acronyms

ART	Asset-referenced token
BCP	Business continuity policy
CASP	Crypto-asset service provider
CSRD	Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (Corporate Sustainability Reporting Directive)
DLT	Distributed ledger technology
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act) and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
EBA	European Banking Authority
EMT	Electronic money token
ESMA	European Securities and Markets Authority
ESAs	European Supervisory Authorities
ESRS	European Sustainability Reporting Standards
ICT	Information and communications technology
ITS	Implementing technical standards
MAR	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC
MAR ITS	Implementing Regulation (EU) 2016/1055 of 29 June 2016 laying down implementing technical standards with regard to the technical means for appropriate public disclosure of inside information and for delaying the public disclosure of inside information in accordance with Regulation (EU) No 596/2014 of the European Parliament and of the Council

MiCA	Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (Markets in Crypto-Assets Regulation)
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II)
NCA	National competent authority
RTS	Regulatory technical standards
UCITS	Undertakings for collective investments in transferable securities
SFDR	Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (Sustainable Finance Disclosure Regulation)

# 1 Executive Summary

## Reasons for publication

The Regulation on Markets in Crypto-Assets (MiCA)<sup>1</sup> requires ESMA, in cooperation with EBA, to prepare regulatory technical standards (RTS) and implementing technical standards (ITS) on a range of mandates for submission to the European Commission.

On 15 October 2023, ESMA published a 'second' Consultation Paper requesting input from stakeholders on ESMA's proposals for six draft RTS and two draft ITS. In the consultation, which closed on 14 December 2023, ESMA received 141 responses, of which 47 were confidential. The non-confidential responses are available on ESMA's website.<sup>2</sup> This Final Report explains how ESMA incorporated stakeholder feedback received in the public consultation.

In parallel, ESMA sought the advice of the Securities and Markets Stakeholder Group (SMSG) established under Regulation (EU) No 1095/2010. The advice submitted by the SMSG in relation to this consultation is included in Annex II.

## Contents

Sections 2 to 7 of the Final Report set out the background of each mandate in this package of eight technical standards as well as ESMA's assessment of feedback received in the aforementioned ESMA public consultation. These technical standards cover (i) sustainability indicators in relation to climate and other environment-related adverse impacts (RTS), (ii) business continuity measures for CASPs (RTS), (iii) pre-and-post-trade transparency for CASP trading platforms (RTS), (iv) record-keeping requirements for CASPs (two RTS), (v) white paper formats and data for their classification in the MiCA register (RTS & ITS), and (vi) disclosure of inside information (ITS).

Section 8 consists of 11 Annexes. Annex I contains the costs/benefit analyses associated with each of the eight draft technical standards in this package. Annex II contains the advice provided by the SMSG. Annex III contains the question-by-question summaries of feedback received from stakeholders. Annexes IV to XI contain the draft technical standards.

## Next Steps

---

<sup>1</sup> Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (OJ L 150, 9.6.2023, p. 40–205).

<sup>2</sup> See: <https://www.esma.europa.eu/press-news/consultations/consultation-technical-standards-specifying-certain-requirements-mica-1st#responses>

The draft technical standards are to be submitted to the European Commission for adoption. In accordance with Articles 10 and 15 of Regulation (EU) 1095/2010, the European Commission shall decide whether to adopt the technical standards within 3 months.

## 2 Sustainability indicators in relation to climate and other environment-related adverse impacts

### 2.1 Background and legal basis

#### **Recital (7)**

*“The consensus mechanisms used for the validation of transactions in crypto-assets might have principal adverse impacts on the climate and other environment-related adverse impacts. Such consensus mechanisms should therefore deploy more environmentally-friendly solutions and ensure that any principal adverse impact that they might have on the climate, and any other environment-related adverse impact, are adequately identified and disclosed by issuers of crypto-assets and crypto-asset service providers. When determining whether adverse impacts are principal, account should be taken of the principle of proportionality and the size and volume of the crypto-asset issued. The European Supervisory Authority (European Securities and Markets Authority) (ESMA) established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council, in cooperation with the European Supervisory Authority (European Banking Authority) (EBA) established by Regulation (EU) No 1093/2010 of the European Parliament and of the Council, should therefore be mandated to develop draft regulatory technical standards to further specify the content, methodologies and presentation of information in relation to sustainability indicators with regard to adverse impacts on climate and other environment-related adverse impacts, and to outline key energy indicators. The draft regulatory technical standards should also ensure coherence of disclosures by issuers of crypto-assets and by crypto-asset service providers. When developing the draft regulatory technical standards, ESMA should take into account the various types of consensus mechanisms used for the validation of transactions in crypto-assets, their characteristics and the differences between them. ESMA should also take into account existing disclosure requirements, ensure complementarity and consistency, and avoid increasing the burden on companies.”*

#### **Article 6(12) of MiCA**

*“ESMA, in cooperation with EBA, shall develop draft regulatory technical standards on the content, methodologies and presentation of the information referred to paragraph 1, first*

*subparagraph, point (j), in respect of the sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts.*

*When developing the draft regulatory technical standards referred to in the first subparagraph, ESMA shall consider the various types of consensus mechanisms used to validate transactions in crypto-assets, their incentive structures and the use of energy, renewable energy and natural resources, the production of waste and greenhouse gas emissions. ESMA shall update those regulatory technical standards in the light of regulatory and technological developments.”*

#### **Article 19 (11) of MiCA**

*“ESMA, in cooperation with EBA, shall develop draft regulatory technical standards on the content, methodologies and presentation of information referred to in paragraph 1, first subparagraph, point (h) in respect of the sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts.*

*When developing the draft regulatory technical standards referred to in the first subparagraph, ESMA shall consider the various types of consensus mechanisms used to validate transactions in crypto-assets, their incentive structures and the use of energy, renewable energy and natural resources, the production of waste and greenhouse gas emissions. ESMA shall update those regulatory technical standards in the light of regulatory and technological developments.”*

#### **Article 51 (15) of MiCA**

*“ESMA, in cooperation with EBA, shall develop draft regulatory technical standards on the content, methodologies and presentation of the information referred to in paragraph 1, point (g), in respect of the sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts.*

*When developing the draft regulatory technical standards referred to in the first subparagraph, ESMA shall consider the various types of consensus mechanisms used to validate transactions in crypto-asset, their incentive structures and the use of energy, renewable energy and natural resources, the production of waste, and greenhouse gas emissions. ESMA shall update the regulatory technical standards in the light of regulatory and technological developments.*

*ESMA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 30 June 2024.*



*Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.”*

#### **Article 66(6) of MiCA**

*“ESMA, in cooperation with EBA, shall develop draft regulatory technical standards on the content, methodologies and presentation of information referred to in paragraph 5 in respect of the sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts.*

*When developing the draft regulatory technical standards referred to in the first subparagraph, ESMA shall consider the various types of consensus mechanisms used to validate crypto-asset transactions, their incentive structures and the use of energy, renewable energy and natural resources, the production of waste and greenhouse gas emissions. ESMA shall update the regulatory technical standards in the light of regulatory and technological developments.*

*ESMA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 30 June 2024.*

*Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.”*

1. Articles 19(1), 51(1) and 6(1) of MiCA respectively introduce disclosure requirements related to the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanisms used to issue a crypto-asset, as part of the white papers for asset-referenced tokens (ARTs), for e-money tokens (EMTs) and for crypto-assets other than ARTs and EMTs. Article 66(5) of MiCA requires crypto-asset service providers to publish on their website information related to the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue each crypto-asset in relation to which they provide services.
2. In turn, ESMA is required by Article 6(2), 19(11), 51(15) and 66(6) to specify the content, methodologies, and presentation of the sustainability indicators in relation to these impacts, taking into consideration the various types of consensus mechanisms used to validate transactions in crypto-assets, covering information on the use of energy and natural resources, the production of waste and greenhouse gas emissions.

## 2.2 Assessment

### 2.2.1 Mandate and relevant features of consensus mechanisms relevant for sustainability impact

#### Background

3. In the Consultation Paper related to these mandates, ESMA noted that the assessment of the sustainability impacts of consensus mechanism is understood as the assessment of the cumulative sustainability impacts of the set of DLT network nodes active in reaching an agreement that a transaction is validated, and that the sustainability impacts of consensus mechanisms are not only linked to the validation of transactions, but also to the use of energy and resources needed to maintain the integrity of the information stored on the ledger.
4. ESMA further noted that the sustainability impact of consensus mechanisms can be anchored in three main features of the DLT network nodes: 1) the energy consumption of each DLT network node; 2) their location; and 3) the devices that each DLT network node uses both to take part in the DLT network and to hold a replica of records of all transactions on a distributed ledger.
5. ESMA's proposal was thus based on the assumption that persons drawing up crypto-asset white papers and CASPs are expected to identify these main features and combine them with relevant datasets, in order to obtain comparable and reliable assessments of the sustainability impact of consensus mechanisms.

#### Feedback to the consultation

6. ESMA's assessment of the mandate for sustainability indicators received wide support from respondents. Suggestions received entailed: i) exempting CASPs providing only a specific sub-set of crypto asset services; ii) introducing a transitional period in light of the challenges in data availability and quality; iii) for multi-layered infrastructures, mandating disclosure on sustainability impacts only at the level of the DLT systems of layer 1 blockchains.
7. A few respondents called for ESMA to provide a taxonomy of the different types of consensus mechanisms, while others provided a long list of these types, noting this list will likely evolve in the future.
8. Some respondents challenged the scope of the RTS and the definition of a DLT network node: they noted concerns about data availability and data quality, as well as more specifically the feasibility of identifying all the nodes for larger and more decentralised networks (e.g. Bitcoin), and called for distinguishing between nodes with different functions (e.g. validating nodes) and for clarifying whether miners will be in scope.

9. A large number of respondents expressed caution on the use of the location of DLT network nodes. At the same time, some respondents were far more optimistic about the possibility of gathering this data, with some going as far as to produce a proof of concept to assess feasibility.

### **ESMA assessment and recommendations**

10. ESMA recognises the proposed disclosures on sustainability impacts require significant efforts from persons drawing up white papers and CASPs. It should however be noted that MiCA itself does not introduce exemptions from sustainability disclosures, neither related to the type, the issuance size or volume or the significance for crypto-assets, nor based on the type of crypto-asset services provided or on the significance for CASPs. Similarly, MiCA does not foresee a delayed application of requirements on sustainability disclosures.
11. As a result, ESMA cannot introduce exemptions for certain crypto-assets or certain crypto-asset services but proposes to build additional proportionality elements via the number of sustainability indicators to be disclosed, and to alleviate the data collection requirements on CASPs - wherever possible (see Section 2.2.3). ESMA also expects market participants to comply with the requirements on sustainability disclosures in line with the application deadline set out in MiCA.
12. ESMA acknowledges the feedback received on the multiple types of consensus mechanisms, the roles performed by DLT network nodes, and the distinction between the validation of a transaction and the issuance or the offer to the public of a crypto-asset. ESMA reflects this feedback in targeted amendments in the recitals of the revised draft RTS but maintains the holistic approach to the assessment of sustainability impacts of consensus mechanisms as proposed. This should ensure that all present and future consensus mechanisms are appropriately captured. In particular this holistic approach captures the sustainability impacts of miners and validators in the assessment, given the pivotal role they play in consensus mechanisms.
13. In light of the general caution on the effective ability to identify the location and the devices used by each DLT network node, ESMA proposes not to mandate the disclosure of indicators largely dependent on the identification of these elements, in particular for the production of waste and for the use of natural resources (see Section 2.2.4). Both these aspects however remain optional indicators that persons drawing up white papers and CASPs may choose to disclose in addition to those they are required to disclose.

## **2.2.2 Coherence, complementarity, consistency and proportionality**

### **Background**

14. In order to foster coherence and comparability between disclosures, ESMA proposed in the Consultation Paper to bundle the mandates on sustainability indicators for crypto-asset white papers and for CASPs' websites into one common RTS.

15. The definitions and concepts in the MiCA sustainability disclosure requirements are, to the extent possible, aligned with and inspired by rules included in CSRD and SFDR, to ensure complementarity and consistency with existing sustainability disclosure requirements, notably as some persons drawing up crypto-asset white papers and CASPs may also be subject to these rules.
16. To ensure proportionality, ESMA proposed that indicators are only made mandatory when they can be considered the most conducive to investor awareness on the impact of consensus mechanisms, with additional indicators identified for optional disclosures. Finally, the draft RTS included the possibility for entities subject to disclosure requirements to benefit from a best effort clause in case of limited data availability.

### **Feedback to the consultation**

17. ESMA's overall approach received positive feedback, but many respondents called for further clarifications or adaptations of the draft RTS, for consistency and proportionality.
18. Several respondents noted that the responsibility for disclosures should lie mainly with persons drawing up white papers rather than CASPs, calling for clarifications on the way sustainability information will be produced and disclosed when a crypto-asset is of relevance for multiple persons subject to the disclosure requirements.
19. A number of respondents called for additional flexibility and proportionality depending on the size of the relevant entities. In particular, some respondents favoured the inclusion of de minimis thresholds (e.g. based on issuance size for ART and EMT) under which persons drawing up white papers and/or CASPs should not be required to disclose information on sustainability impacts.

### **ESMA assessment and recommendations**

20. ESMA shares the general view from respondents that the persons drawing up the white papers (offerors, persons seeking admission to trading, issuers, or CASPs operating the trading platform) are better placed than other CASPs to assess the sustainability impacts of the crypto-assets. ESMA also notes the concerns that disclosure requirements in white papers and on the websites of CASPs introduced separately in MiCA could in effect lead to multiple versions of the assessment of sustainability impacts for each crypto-asset.
21. To remedy these concerns, in addition to the clarity and harmonised format introduced by the draft RTS themselves, and to the call for coordination between market participants, ESMA proposes that CASPs are explicitly encouraged to use white papers to fulfil their website disclosure requirements where available. In this way, ESMA also anticipates that the white papers (including the information on sustainability impacts) that a CASP operating a trading platform will draw up pursuant to Article 5(2) of MiCA where no white paper already exists, can also be used by other CASPs to fulfil their website disclosure requirements.

22. Past the transitional period provided for under Article 143 of MiCA (during which it can be anticipated that there might be cases of CASPs already authorised under the definitive MiCA regime providing services in relation to crypto-assets whose issuers are not yet required to produce a white-paper), ESMA expects that there will be few cases of a CASP falling under the scope of Article 5 of the draft RTS without there being an existing white paper under Article 4 of the draft RTS. In such a case however, the CASP would need to disclose on their website information on sustainability impacts as required by Article 5 of the draft RTS, despite the absence of a white paper. ESMA therefore reiterates its call for voluntary cooperation between CASPs, especially CASPs operating a trading platform, to ensure coherence across all information made available to investors on sustainability impacts.
23. MiCA does not foresee exemptions in sustainability disclosure requirements for certain crypto-assets or crypto-asset services other than those arising from the aforementioned exemptions stemming from Article 4 of MiCA. However, ESMA proposes to introduce additional proportionality in the revised draft RTS, aiming to reduce the reporting burden in relation to all crypto-assets, with a particular focus on crypto-assets issued on DLTs with a smaller energy consumption in absolute terms, and in turn for all CASPs providing services in relation to these crypto-assets, with a particular focus on those whose services are less likely to require an investor to independently compare between consensus mechanisms.
24. In more detail, ESMA achieves this substantial reduction of the reporting burden by:
  - i. turning indicators on the production of waste and the use of natural resources (indicators stemming from the SFDR framework) from mandatory to optional for all reporting entities considering on one hand the reporting burden on reporting entities in view of the currently limited data availability, and on the other, the incremental benefit of these indicators for investors: this results in a 40% reduction in the number of mandatory indicators overall;
  - ii. introducing a new proportionality threshold, based on the annual energy consumption of the consensus mechanism used to issue the crypto-asset at hand, and requiring the disclosure of only one mandatory key indicator on energy consumption for crypto-assets below the threshold, while requiring detailed disclosures with five supplementary key indicators only for crypto-assets issued on DLTs above the energy-based proportionality threshold: this results in a 90% reduction in the number of mandatory indicators for these crypto-assets;
  - iii. requiring the disclosure of only one mandatory key indicator on energy consumption for crypto-assets below the energy-based proportionality threshold: this results in a 90% reduction in the number of mandatory indicators for these crypto-assets
  - iv. exempting CASPs other than those operating a trading platform or providing the services of exchange of crypto-assets for funds or for other crypto-assets from disclosures other than the one mandatory key indicator on energy consumption.

25. The below table summarises the approach in revised draft RTS compared to the approach proposed in the Consultation Paper.

Entity in scope	Draft RTS	Revised draft RTS
<b>Person drafting crypto-asset white paper</b>	10 mandatory indicators for all crypto-assets	1 mandatory key indicator and 5 supplementary key indicators for crypto-assets whose consensus mechanism consumes more than 500 000 kWh per year  1 mandatory key indicator for crypto-assets whose consensus mechanism consumes less than 500 000 kWh per year
<b>CASPs providing one or more of the following services:</b>  - Operating a trading platform,  - Exchanging crypto-assets for funds or  - Exchanging crypto-assets for other crypto-assets	10 mandatory indicators for all crypto-assets in relation to which services are provided	1 mandatory key and 5 supplementary key indicators in relation to all crypto-assets whose consensus mechanism consumes more than 500 000 kWh per year,  1 mandatory key indicator in relation to crypto-assets whose consensus mechanism consumes less than 500 000 kWh per year
<b>CASPs only providing services other than those listed above</b>	10 mandatory indicators for all crypto-assets in relation to which services are provided	1 mandatory key indicator for all crypto-assets in relation to which services are provided

### 2.2.3 Data availability and reliability

#### Background

26. In the Consultation paper, ESMA proposed that, initially, disclosures for both new and existing crypto-assets can be based on estimates, considering that sustainability data with respect to consensus mechanisms may not be fully available when MiCA applies.



27. ESMA also proposed that the use of third parties to review sustainability disclosures is indicated in white papers and on CASPs' websites, in line with the approach applicable to disclosures related to the taxonomy on EU sustainable activities in the SFDR RTS<sup>3</sup>.
28. In addition, ESMA encouraged persons responsible for drawing up crypto-asset white papers and CASPs to increase their coordination in anticipation of the application of MiCA, in order to foster consistent implementation of the sustainability disclosures across the board, notably when the same crypto-asset is admitted to trading on different trading platforms.

### **Feedback to the consultation**

29. The vast majority of respondents strongly supported the use of estimates, with some suggesting allowing them only for crypto-assets' issuance, or for a limited time period, while others asked for additional guidance on the notion of 'best efforts', limited data availability' and on what constitutes 'readily available [information]' and 'reasonable assumptions' in Article 4(8) of the draft RTS.
30. Some respondents remarked the high costs due to the collection of data and to using third-party providers, noting that the use of estimates would involve costs as well. Some also asked whether ESMA could provide a list of data sources deemed reliable or standardised sustainability data for certain crypto-assets. Finally, a few respondents challenged the requirements to review the information regularly and at least annually.

### **ESMA assessment and recommendations**

31. ESMA continues to acknowledge that the challenges related to data availability and reliability are particularly acute for crypto-asset markets, while observing that transparency is often mentioned as one of the main benefits of the on-chain structure of crypto-assets. ESMA also notes that since the adoption of MiCA, and in particular since the publication of the Consultation Paper, the increased attention to crypto-assets' sustainability impacts has been accompanied by more granular data on these impacts, including for crypto-assets such as Bitcoin, despite the distributed nature of the underlying consensus mechanisms.
32. ESMA had already introduced in the draft RTS a significant margin of flexibility compared to other frameworks applicable to sustainability disclosures, including an explicit mention of the use of estimates as part of a general 'best efforts' clause. In the revised draft RTS, ESMA notes that the best effort clause is only conditioned to the disclosure on a few information items, rather than all of these additional disclosures.

---

<sup>3</sup> Delegated Regulation (EU) 2022/1288 of 6 April 2022 supplementing Regulation (EU) 2019/2088 of the European Parliament and of the Council, ELI: [http://data.europa.eu/eli/reg\\_del/2022/1288/oj](http://data.europa.eu/eli/reg_del/2022/1288/oj)

33. ESMA considers that the part on data use in the answer provided by the European Commission in Q&A VII.1 in the Consolidated questions and answers on the SFDR and the CDR 2022/1288<sup>4</sup> could serve as guidance on what constitutes ‘readily available [information]’ for the MiCA sustainability disclosures and may consider issuing additional level 3 guidance. For additional background, ESMA wishes to draw respondents’ attention to its recent publication on the ‘Concept of estimates across the EU Sustainable Finance framework’<sup>5</sup>.
34. At this stage, it is not envisaged to clarify further the definition of ‘reasonable assumptions’ as such clarification at an early stage of implementation may curtail stakeholders’ ability to fulfil the disclosure requirements.
35. In addition, ESMA wishes to clarify that disclosures on sustainability impacts are mandatory requirements applicable to persons drawing up white papers and to CASPs, with no mandate in MiCA for ESMA to certify data sources or to produce standardised sustainability data.
36. Similarly, the use of third-party entities for verification, of third-party data providers or of external experts is not a mandatory requirement, but an option that persons drawing up the white papers and CASPs can use to fulfil their disclosure requirements.
37. Finally, the requirement to review sustainability indicators at least annually and in case of material changes is in line with the review requirements applicable to the general content of white papers and results from the ‘average per year’ approach for most of the sustainability indicators.

## 2.2.4 Indicators, methodologies, and presentation of the information

### Background

38. In the Consultation Paper, ESMA proposed a targeted set of mandatory disclosures with a limited number of quantitative metrics on the consumption of energy, scope 1 and scope 2 GHG emissions, and the production of waste, together with a qualitative statement on the impact of use of equipment by DLT network nodes on natural resources. ESMA also provided optional indicators covering granular information on the energy mix used, on scope 3 GHG emissions, on the generation and recycling of all types of waste and the waste intensity of each transaction, and on the use and recycling of water by DLT network nodes. These optional indicators could be made mandatory in the medium term if they are considered to improve investor awareness.
39. In the short-term, as noted in the Consultation Paper, ESMA expects that the certainty provided in the draft RTS should enhance the availability of sustainability data in relation

---

<sup>4</sup> [https://www.esma.europa.eu/sites/default/files/2023-05/JC\\_2023\\_18\\_-\\_Consolidated\\_JC\\_SFDR\\_QAs.pdf](https://www.esma.europa.eu/sites/default/files/2023-05/JC_2023_18_-_Consolidated_JC_SFDR_QAs.pdf)

<sup>5</sup> [https://www.esma.europa.eu/sites/default/files/2023-11/ESMA30-1668416927-2548\\_Note\\_Use\\_of\\_estimates\\_and\\_equivalent\\_information.pdf](https://www.esma.europa.eu/sites/default/files/2023-11/ESMA30-1668416927-2548_Note_Use_of_estimates_and_equivalent_information.pdf)



to crypto-assets ahead of the application of MiCA requirements by end 2024. In the medium-term, ESMA intends to suggest revisions to the RTS incorporating new findings in a fast-evolving field of research, and conclusions from forthcoming Commission reports. This dynamic approach will incrementally increase the scope of sustainability disclosures for crypto-assets.

40. While a standardised calculation methodology is not yet available, the first version of the draft RTS already catered for a harmonised approach following the calculation guidance given in the draft ESRS. ESMA may explore additional guidance on recommended methodologies and data sources based on the feedback received during the consultation.
41. Finally, ESMA proposed including in the draft RTS general principles on the presentation of the information on the websites of CASPs, as well as a common template for sustainability disclosures (in the Annex of the draft RTS), to ensure comparability across CASPs and foster investor understanding. This template includes a specific focus on the key indicators described above.

### **Feedback to the consultation**

42. Generally, several respondents agreed with ESMA's practical approach to assessing sustainability impacts of the consensus mechanism, with some supporting a phased approach, starting with indicators for which there is higher data availability. A number of respondents indicated a wish to include their perceived positive environmental aspects of certain consensus mechanisms. Another suggestion was to not measure energy per transaction but per block.
43. Regarding the proposed indicators, some respondents find they are conducive of investors' awareness, while others expressed concerns with regard to their amount and complexity, and with the availability and quality of data. Mostly, respondents showed preference for limiting the number of mandatory indicators, focusing on the consistency and clarity of a few of them, keeping the others as optional. Some respondents agree with making optional indicators mandatory but ask for a post-implementation review.
44. Respondents provided additional suggestions regarding the principles for the presentation of information, with the main comment being about amending Article 4 and the Annex of the draft RTS with regarding the obligations for issuers. Other suggestions entailed adding fields for positive impact, qualitative information and executive summary, and avoiding splitting emissions into scopes to avoid confusion.
45. Many respondents did not show support for the use of the ESRS for calculation guidance, as it is also quite new for firms subject to CSRD requirements, and it may bring additional challenges for entities subject to MiCA requirements. Additional suggestions were: (i) adopting an issuer-centric approach base on SFDR; and (i) implementing dual reporting based on location- and market-based reporting. The general plea was that the RTS be designed with a balance between offering specific guidance and allowing for flexibility.

## **ESMA assessment and recommendations**

46. In line with the mandate in MiCA, ESMA has considered and included in its proposed draft RTS a large number of sustainability indicators covering the use of energy, renewable energy and natural resources, the production of waste and greenhouse gas emissions. As mentioned above, ESMA proposes that indicators on the production of waste and the use of natural resources are optional rather than mandatory at this stage, considering that they may require a higher effort for data collection, especially in the initial period, and that they are less conducive to investor awareness compared to the indicators on energy consumption. In accordance with the mandate, in the future ESMA may also consider making these indicators mandatory in light of technological developments and increased availability of data.
47. In the revised draft RTS, ESMA updates the format of the disclosure template, in order to align it with the proposed format for white papers in the relevant revised draft RTS. This format does not allow for information other than the information listed in Tables 2, 3 and 4 of the draft RTS to be disclosed, but such additional information may be disclosed by persons drawing up white papers and CASPs alongside the mandatory disclosures, e.g. in their marketing documents.

## 3 Measures to ensure continuity and regularity in the performance of crypto-asset services

### 3.1 Background and legal basis

#### Article 68 (10) (a) of MiCA:

“ESMA shall develop draft regulatory technical standards to further specify:

(a) the measures ensuring continuity and regularity in the performance of the crypto-asset services referred to in paragraph 7;

[...]

ESMA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 30 June 2024.

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.”

48. Chapter 2 of Title V in MiCA lists obligations for all crypto-asset service providers (CASPs), including specific governance arrangements listed under Article 68. These governance arrangements fall into the wider organisational requirements for CASPs described in Recital 81 of MiCA, which are aimed at ensuring market integrity.
49. As part of these governance arrangements for CASPs, Article 68(10)(a) of MiCA mandates ESMA to develop regulatory technical standards (RTS) to further specify the “measures” that CASPs must take to ensure continuity and regularity in the performance of the crypto-asset services referred to in paragraph 7 of the same article.
50. Paragraph 7 of Article 68 imposes requirements on CASPs to take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services by employing appropriate and proportionate procedures to ensure resilient and secure ICT systems, as required by Regulation (EU) 2022/2554 (henceforth DORA). They must establish a Business Continuity Policy (BCP), which includes ICT business continuity plans as well as ICT response and recovery plans that aim to ensure—in case of interruption to their ICT systems and procedures—the preservation of essential data and functions, and the maintenance or timely recovery of crypto-asset services.

### 3.2 Assessment

#### 3.2.1 Definitions in the draft RTS

## Background

51. In the draft RTS published in the Consultation Paper, ESMA introduced two new definitions not found in Level 1 of MiCA. Those definitions, in Article 1 of the RTS, are for (i) 'critical and important functions' of the CASP and (ii) 'permissionless distributed ledger technology'. In the CP, ESMA asked whether stakeholders agree with both the necessity and the content of the two definitions.
52. ESMA adapted the definition of 'permissionless distributed ledger technology' from the Financial Stability Board (FSB) definition found in the 2022 consultative document on crypto-asset supervision.<sup>6</sup> The FSB definition itself builds from accepted principles conceived by the International Organisation for Standardisation (ISO). The term, 'permissionless', is also already widely understood by market participants in the crypto industry to mean publicly accessible DLTs (such as Ethereum) that do not gatekeep access to the validator network. ESMA considers this definition necessary to clarify the procedures for external communication with clients in Article 4(2)(e) and the general principal on proportionality in Article 6 of the draft RTS.
53. The definition of 'critical and important functions' (a term that does not have any ICT-specific connotations) is borrowed from DORA Article 3, point 22. It allows the RTS to streamline how we refer to the broad range of non-ICT business and operational functions a CASP may employ to maintain the availability and integrity of their services.

## Feedback to the consultation

54. Although most respondents supported the inclusion of a specific definition to capture the concept of public, permissionless DLTs, much of the support was conditional on fine-tuning the definition to make it clear that CASPs would require 'effective control' of the DLT to ultimately be liable for any service disruptions or other operational incidents caused by the DLT. Respondents who objected to the definition said the reference to 'core services' would introduce a more specific notion of 'control' than what is provided in Level 1, jeopardizing a CASP's ability to comply with the business continuity measures in the draft RTS.
55. Objections to the reference to 'core services' in the definition came from several respondents who expressed concerns that this term would inadvertently bring many permissionless DLTs using ancillary value-added services (such as RPC node providers) into the scope of the regulation. Respondents argued MiCA does not intend to bring into scope the open-source software projects that often serve as user-friendly access points to DLT-based services.
56. As it relates to a CASP's liability to clients for services using permissionless DLT and the notion of 'effective control' over that DLT, several respondents argued that the

---

<sup>6</sup> FSB, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative document, 11 October 2022 (See Annex 1 here: [link](#))

permissionless vs. permissioned distinction in the draft RTS 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.

57. One respondent pointed out that the definition in the draft RTS does not match exactly the definition used by the FSB (noting its proximity instead to the ESMA Guidelines on standard forms, formats and templates to apply for permission to operate a DLT Market Infrastructure).<sup>7</sup> Another respondent suggested the addition of a definition for 'permissioned DLT' to make it clearer what the RTS is defining 'permissionless' DLT against.
58. Most respondents agreed with the inclusion of the definition of 'critical or important functions' in the draft RTS, calling the consistency with DORA a welcome addition. Many caveated that, as with DORA, CASPs should be able to identify their own critical or important functions for the purposes of the RTS, in line with the principle of proportionality. However, two respondents cited the definition of 'critical functions' found in Article 2(1)(35) of Directive 2014/59/EU (the Bank Recovery and Resolution Directive, BRRD<sup>8</sup>) as a more appropriate alternative.

### **ESMA assessment and recommendations**

59. Considering the objections from respondents in the consultation to the inclusion of the concept of 'core services' in the definition of 'permissionless DLT', ESMA has removed it from the definition. The ambiguity around this concept of 'core services' could have unintentionally excluded many DLTs that the market and regulators would consider public, permissionless networks from qualifying as permissionless. Its removal would also align the definition closer with the FSB definition, as requested by one respondent. Another minor change to the definition is the removal of 'technology' from the term itself. Although not requested in the consultation feedback, ESMA has made this revision to clarify that we are not dealing with an abstract technology, rather, it is a commonly found ICT infrastructure deployed by many CASPs in the market today.
60. At the same time, ESMA has modified Recital 3 of the draft RTS to clarify that permissionless DLT would constitute a type of distributed ledger that the CASP 'does not control' in accordance with the second subparagraph of Article 75(8) of MiCA. This reference to the Level 1 concept of control would provide a basis for how supervisors should treat permissionless DLTs in assessing compliance with the draft RTS. Although ESMA acknowledges that this revision introduces another concept (i.e., 'control') that may contribute to further uncertainty for market participants, the direct association between permissionless DLT and the liability exemption in Article 75(8) should be

---

<sup>7</sup> ESMA, Final Report - Guidelines on standard forms, formats and templates to apply for permission to operate a DLT Market Infrastructure, 15 December 2022 ([ESMA70-460-206](#))

<sup>8</sup> OJ L 173, 12.6.2014, p. 190–348 ([link](#))

sufficient to clarify the intent of all provisions involving permissionless DLT in the draft RTS.

61. To further clarify the concept, ESMA considers that a DLT would meet this standard for 'no control' found in Level 1 when the relationship between the CASP and the DLT adheres to two principles: (i) the DLT is not owned or operated by the CASP. In this case, a controlling share of DLT network nodes or other governance mechanics of the distributed ledger by the CASP would constitute control. And (ii) the CASP's use of the DLT is not subject to any written (i.e., contractual) agreement pursuant to Article 73(3) of MiCA nor does it constitute an 'ICT third-party service provider' relationship per the definition in DORA. This test acknowledges that a CASP can impose 'control' over a DLT (and therefore meet the business continuity requirements in the RTS) through the existence of a contractual relationship (e.g., a third-party provider relationship with a private or permissioned DLT service provider). With this clarification, the meaning of permissionless DLT in the draft RTS should be widely understood. In applying the definition to CASP operating models, competent authorities may choose to assess the validity of 'permissionless' claims on a case-by-case basis as part of their supervisory duties.
62. For the definition of 'critical and important functions', given the broad support and utility of the term to the draft RTS, ESMA intends to keep it as currently drafted. Considering the shared subject matter with DORA, ESMA believes the current definition is superior to the BRRD definition proposed by some respondents. References to disruptions to the real economy and financial stability in the BRRD definition render it inappropriate in the narrow context of CASPs.

### **3.2.2 External communication in disruptions to services using distributed ledger technology the CASP does not control**

#### **Background**

63. In the draft RTS, ESMA includes provisions that would acknowledge the differences between public / permissionless and private / permissioned DLTs in the context of business continuity. ESMA considers these provisions necessary for investor protection purposes because services involving DLTs that a CASP does not control would not be subject to the business continuity measures in this RTS (nor would they be captured under DORA as an 'ICT third-party service provider').
64. One such provision based on this reasoning is Article 4(2)(d) (and the associated Recital 3), which would require CASPs to communicate externally with their clients in the event of a service disruption involving a DLT the CASP does not control. As part of this obligation, the provision requires CASPs to provide regular communication to their clients about the cause of the disruption to the DLT, when the affected CASP service is expected to resume (where available), whether their funds are at risk due to the disruption, and how the distributed ledger will be brought back online (e.g., a fork, or a roll-back to a

previous timestamp). This last piece of information is important for clients whose transactions may be reversed ex-post despite already being executed (or fail to settle on-chain).

65. Although external communication is not explicitly mentioned in the mandate, ESMA believes this information would ensure a more orderly return to service once the incident is resolved and should constitute an important feature of a CASP's business continuity plan. This provision is inspired by similar measures for external communications with clients for major ICT-related incidents found in Article 11(2)(d) and Article 14 of DORA.
66. ESMA also justified this inclusion in the RTS as part of the duties for CASPs enumerated in Article 66 of MiCA to act in the best interests of clients. As part of this obligation, ESMA believes CASPs that intend to conduct their services on DLTs the CASP does not control should make their clients aware of the risks that this entails at the point when their clients first access those services. In the same spirit of disclosure, ESMA would also encourage CASPs to explain to their clients that their liability does not extend to DLTs they do not control.
67. In the Consultation Paper, ESMA asked stakeholders to provide their views on whether the new 'timely communication' obligation was appropriate for the mandate and if it can be considered a measure ensuring business continuity.

### **Feedback to the consultation**

68. Respondents had mixed views about the proposed provision on 'timely' communication with clients in Article 4(2)(e) in the event of service disruptions involving a DLT the CASP does not control. Those in support said it would not hinder innovation or the use of such DLTs in CASP services. Those who objected said it would create a double standard for different types of technology and risked undermining the principle of tech neutrality.
69. Several respondents asked for clarification about whether the information would be required for all aspects of the DLT experiencing a disruption or just for those disruptions that affect the services provided by the CASP itself. This is clear in the provision itself, which only refers to CASP services. However, such communications would inherently depend on the status of the disrupted DLT for some of the information, specifically, when the services can be expected to resume.
70. In ensuring accurate and helpful communications from the CASP, one respondent highlighted two elements of importance: (i) the significance of the impact, and (ii) the preciseness of the information being communicated. On the preciseness, several respondents further noted that CASPs may have limited access to information about DLT infrastructures they do not control, and therefore should only have to estimate time to resumption of their services 'to the best of their ability' or 'where possible'.
71. Assuming that the CASP has no control over the availability or operations of the relevant permissionless DLT, other than as a participant in the relevant system, then it is unlikely



to be in a position to report – during the time of nonavailability – on the time-to-recovery, the reasons and the impact of the incident, or the risks to clients' funds or crypto-assets held on their behalf. What it can and should do is take reasonable measures to secure the property of its clients, monitor the situation with the permissionless DLT, and provide best-effort reporting to clients on the situation.

72. Several respondents questioned whether the same measures for external communications should be applicable for all disruptions to the CASP's service, regardless of the type of ICT or non-ICT critical or important functions at the source of the disruption. They argued that identifying only DLTs the CASP does not control for the purpose of communication with clients would not be tech neutral and concerns a type of ICT infrastructure that falls outside the scope of MiCA and DORA.
73. The ECB's Markets Infrastructure Payments Committee (MIPC) expressed support for the measures for external communication and suggested extending the requirement by borrowing language from the CP about ensuring CASPs make their clients aware that their liability does not extend to services using DLTs the CASP does not control (and making this disclosure mandatory). However, as the discussion on liability does not fit within the business continuity mandate in MiCA, it cannot be included in this RTS. That said, ESMA would like to re-emphasise the usefulness of such a disclosure to clients by CASPs as part of their obligations under Article 66 of MiCA.

### **ESMA assessment and recommendations**

74. On the point about tech neutrality, ESMA reiterates that CASPs will be subject to DORA and hence would already be responsible for external communications with clients for service disruptions involving their in-house ICT infrastructure and ICT service provided by third-parties, per Article 14 of that regulation. So, the inclusion of this same measure for DLTs the CASP does not control would support the principle of tech neutrality.
75. The concern raised by respondents of CASPs being unable to meet certain aspects of the requirement due to *incomplete access* to information about a DLT they do not control is valid. As such, ESMA proposes the addition of 'where available' to the text in subpoint (e) of Article 4(2) of the draft RTS in reference to the estimated time to resumption of CASP services (which may depend on when the DLT is brought back online). As for the *preciseness* of the information, this can only be provided on the best abilities of the CASP and should be understood as an implicit objective of any such communications.

### **3.2.3 Measures for business continuity management**

#### **Background**

76. The four articles specifying the business continuity management requirements in the draft RTS follow the standardised playbook seen in other sectoral regulations (e.g., MiFID II). These include (i) organisational arrangements, (ii) the business continuity



policy (including independent auditing), (iii) business continuity plan, and (iv) periodic review and testing of the business continuity policy.

77. Article 2 of the draft RTS on organisational arrangements requires CASPs to have dedicated resources for their business continuity arrangements, including personnel capable of discharging the duties allocated to them as laid out in Article 68(5) of MiCA. Included in these organisational arrangements is the role of the CASP's management body, which must endorse and regularly review the business continuity policy. The article further specifies MiCA Level 1 by requiring the management body to review the business continuity policy on at least an annual basis (specifying "periodically" in Article 68(6) of MiCA). The article also requires CASPs to establish adequate procedures to ensure that updated information on the business continuity policy is transmitted to all relevant internal staff and external stakeholders.
78. In the CP, respondents were asked whether the RTS should specify that CASPs are required to establish a business continuity management function. In addition, respondents were asked whether the RTS should include requirements concerning other additional organisational measures for specific CASP services beyond those listed in the RTS.

### **Feedback to the consultation**

79. Several respondents indicated that mandating a business continuity management function would be too prescriptive relative to the mandate. The concerns centred around the proportionality of requiring a business continuity management function. For example, if such a measure were to be included in the RTS, respondents suggested an exemption for microenterprises per precedent in DORA or that it should apply only to significant CASPs.
80. While there was significant resistance to imposing a requirement for a *management function* dedicated to business continuity, a high number of respondents supported the notion that there should at least be *resources* dedicated to business continuity. Respondents generally noted that the level of those resources and their specific form should be subject to some flexibility and proportionality. Along these lines, there was one suggestion to allow CASPs that are part of a group structure in which a business continuity function already exists somewhere within the organisation to leverage on those resources.
81. A significant majority of the respondents indicated that no further organisational measures should be considered. Several responses mention that further measures would potentially create a disproportionate administrative burden on CASPs, in particular for smaller entities. Here there was a suggestion to follow precedent in DORA by exempting microenterprises from the more burdensome requirements. One respondent indicated there might be other relevant organisational measures but that the consideration of such measures should be left to CASPs themselves and subject to proportionality considerations.

82. One response mentioned the need for organisational measures specifically for CASPs which rely on third parties for crypto-asset custody services. The response included proposed rules and standards for the selection of such third parties including service level agreements, incident response procedures, third-party dependencies, change management, etc.
83. Another response called for further organisational measures but did not specify what these measures should entail. Rather the respondent emphasised more generally that there might be a need for measures that take into account specific risks of crypto assets related to client asset protection, compliance and transaction monitoring, and cybersecurity measures beyond DORA requirements.

### **ESMA assessment and recommendations**

84. The principle of proportionality is already well embedded in the draft RTS. As such, no further amendments have been made in response to the comments with respect to the application of the various obligations in a manner that is proportional to the different types of enterprises within its scope. The draft RTS in its current form gives sufficient room to consider proportionality.
85. Given that most respondents felt that including further organisational measures would be disproportionate, the RTS will not be amended to expand upon the organisational measures currently covered. The suggestions that were offered for more specific organisational measures, e.g., for CASPs relying on third-parties in their custody services is likely to push the limits of proportionality and risks going beyond them.
86. The draft RTS does not require the establishment of a dedicated business continuity management function within the CASP. However, the draft RTS does require CASPs to devote “adequate” resources to business continuity, leaving the form in which such resources are dedicated to the discretion of the CASP. Such resources may be sourced from existing functions, including the control function CASPs will be required to implement as part of the requirement in Article 6(4) of DORA. The only post-consultation modification to this Article in the draft RTS is a small addition to the procedures in Article 2(3), which now specifies that CASPs should establish ‘effective communication channels’ for the smooth implementation of their business continuity plans and for circumstances in which execution of those plans would require outreach to clients or other external stakeholders (NCAs, other CASPs). This notion of ‘effective channels’ mirrors the approach in [*Delegated Regulation xxx/xxx RTS conflict of interest*].

### **3.2.4 Independent assessment of the testing of business continuity plans**

#### **Background**

87. Article 4 of the draft RTS requires CASPs to establish general business continuity plan(s) for the services that depend on their (non-ICT-related) critical or important functions. As part of the business continuity planning, CASPs are required to identify risk scenarios,

establish recovery time and recovery point objectives for their systems, as well as plan for the relocation or back-up of their critical business functions in the event of a disruption.

88. In the draft RTS shared in the CP, ESMA included in paragraph 4 of Article 4 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 broad business continuity measures (policy, plans and procedures).

### **Feedback to the consultation**

89. Most respondents objected to the proposed paragraph 4 of Article 4. Objections to the provision considered it outside of the mandate, especially when looking at precedents for governance of business continuity measures in other sectoral regulation. Those that supported the proposal reasoned that since CASPs would be subject to DORA, they should already have an audit function as part of the governance requirements for 'three lines of defence' (proportional to their size, complexity and risks). Some respondents also noted that this assessment could be conducted by an intra-group entity with an auditing function and called for flexibility in how to fulfil the obligation.
90. Some respondents advocated for the possibility to have an external auditing, including for smaller or standalone CASPs. This was already envisioned in paragraph 4 of Article 4 with the inclusion of 'independent assessor' although it may not have been clear as drafted that this refers to an external third-party auditor. Other respondents said that the responsibility for confirming the results of the testing of business continuity plans should be reserved only for the management body of the entity, not external auditors.
91. Additionally, one respondent underscored the complexities of testing business continuity plans that incorporate procedures for recovering services that use a DLT the CASP does not control. Such testing, this respondent said, would require a complex multi-party strategy in circumstances in which a service level agreement may not exist to create a contractual obligation for cooperation on business continuity testing. Although this comment is valid, it concerns Article 5 on 'periodic testing'—not auditing of the results of those tests as envisioned in the provision in question here. Finally, there was a suggestion to introduce a transition period of one year for this requirement followed by audits every two years afterwards.

### **ESMA assessment and recommendations**

92. ESMA proposes the removal of the specific paragraph in Article 4(4) of the draft RTS that was referenced in this question presented in the consultation. After further assessment, and taking into consideration feedback from the consultation, ESMA no longer considers this provision necessary for CASPs to fulfil their requirements under the mandate. The testing of the business continuity plans envisioned in Article 5 of the draft RTS should be sufficient to ensure the proper execution of those plans and their revision where necessary. Requiring an independent assessor to review the management body's

oversight of the implementation of the organisation's business continuity plans could have the adverse effect of pulling resources away from other mission critical business continuity processes.

### **3.2.5 Principle on risk considerations and risk self-assessment**

#### **Background**

93. In Article 6 of the draft RTS, ESMA proposes a general principle on risk considerations which is meant to specify the language found in Article 68(6) and (8) on the “scale, the nature and range of crypto-asset services provided”. In particular, the principle 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.
94. Paragraph 2 of Article 6 builds on this principle with a mandatory ‘self-assessment’ to be completed by the CASP. The self-assessment, a concept borrowed from MiFID, is meant to (i) ensure that CASPs are taking stock of the risk factors that may cause or prolong interruptions in the availability of their services (and affect the execution of their business continuity plans), and (ii) provide supervisors with a tool to assess if CASPs are implementing business continuity procedures commensurate with the risks they pose. The assessment would have the added benefit of allowing supervisors to compare these risk factors and their associated mitigation procedures between CASPs for a better understanding of how to implement proportionality in supervision.
95. The criteria of this self-assessment are available in the Annex of the RTS. In the CP, ESMA asked stakeholders for their views on the risk consideration principle and the self-assessment as well as whether they consider other criteria suitable to further refine the CASP's assessment of its own risk and complexity factors.

#### **Feedback to the consultation**

96. The general principle on risk considerations in Article 6 of the draft RTS received broad support from respondents. Some comments suggested to clarify explicitly that the obligation for a self-assessment stems from Article 68(8) of MiCA. Others suggested to avoid new definitions, such as ‘permissionless DLT’, to maintain a ‘tech-agnostic’ approach in the RTS. This latter comment is addressed in Section 3.2.1 on definitions.
97. On the self-assessment, most respondents supported the proposal and the criteria listed in the Annex (with several caveats and requests for extensions). Only one respondent objected to the proposed self-assessment, questioning whether it was in the Level 1 mandate. This respondent argued that it would be duplicative to the obligations in their business continuity plans and instead suggested that the RTS allow CASPs to choose their own criteria for the self-assessment. There was another suggestion to extend the minimum timeframe for the self-assessment from at least annually to bi-annually to ease the burden on CASPs.

98. Additional criteria suggestions included: a criterion for the *type* or *volatility* of the crypto-assets that are held in custody (under the assumption that some are riskier than others), the inclusion of ESG-based criteria, and the scale of personal data collected.
99. To acknowledge for circumstances in which the CASP may not be able to fulfil one of the criteria (e.g., because they are not providing the relevant service or do not use certain ICT infrastructure in their services), one respondent suggested the addition of 'if any' to clarify that there would be no obligation to answer.
100. The ECB (MIPC) also weighed in on the criteria in the Annex, suggesting they account for the *types* of smart contracts used or deployed by CASPs in addition to the overall number. The rationale is that complexity could depend not only on the smart contracts directly deployed and maintained by a CASP but, more broadly, by all smart contracts used in the execution of services (including those smart contracts that are deployed and maintained by third-party developers providing their technical services to the CASP). Another proposed edit to the criteria came from several respondents who called for removing sub-point c(v) and edit c(vi) to account for other means of securing clients' access to their crypto-assets under the safekeeping obligation.

#### **ESMA assessment and recommendations**

101. ESMA considers the proposed additional criteria out of scope of the mandate for business continuity because they either introduce unrelated elements into the RTS (i.e., it is not clear how ESG factors would illuminate business continuity risks) or they would invite the creation of a 'risk-based taxonomy' for crypto assets, which would be outside of the mandate and controversial to implement in practice because crypto-asset risk indicators are not static over time.
102. To the suggestion that CASPs be allowed to determine their own self-assessment criteria, ESMA does not consider this will be helpful for supervisors in practice. For the self-assessment to be effective, it is necessary to have standard and common criteria for CASPs, providing supervisors with a baseline for comparison.
103. Finally, ESMA has included two additions in the Annex criteria on the basis of the feedback shared by ECB's MIPC and other stakeholders. These include the reference to (i) the *type* of smart contracts deployed and maintained by the CASP, and (ii) the safekeeping of clients' private keys *and other means* of accessing crypto-assets.

## 4 Pre-and-post-trade transparency

### 4.1 Background and legal basis

#### **Article 76 (16) (a) of MiCA:**

*ESMA shall develop draft regulatory technical standards to further specify:*

*(a) the manner in which transparency data, including the level of disaggregation of the data to be made available to the public as referred to in paragraphs 1, 9 and 10, is to be presented;*

*[...]*

*ESMA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by 30 June 2024.*

*Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.*

104. Article 76 of the Markets in Crypto-Assets Regulation (MiCA) sets out the operating conditions of trading platforms for crypto-assets (hereafter also referred generally as trading platforms) operated by crypto-assets service providers (CASPs). In particular, Article 76(1) sets out that trading platforms should lay down, maintain, and implement clear and transparent operating rules for the trading platform they operate.
105. In addition, regarding pre-trade transparency, Article 76(9) requires trading platforms to make public any bid and ask prices and the depth of trading interests at those prices which are advertised through their trading platforms. The CASPs concerned are required to make that information available to the public on a continuous basis during trading hours.
106. Finally, regarding post-trade transparency, Article 76(10) requires trading platforms to make public the price, volume and time of the transactions executed in respect of crypto assets traded on their trading platforms. They are required to make details of all such transactions public as close to real-time as technically possible.
107. Article 76(16)(a) requires ESMA to develop an RTS specifying the manner in which transparency data, including the level of disaggregation of the data to be made available to the public as referred to in paragraphs 1, 9 and 10 of Article 76, is to be presented.
108. This empowerment under Article 76(16)(a) of MiCA includes two different dimensions that should be considered separately. The first dimension relates to transparency data and how this data should be presented, i.e. what details should be published by trading



platforms in relation to crypto assets. The transparency data in this context should distinguish between pre-trade and post-trade transparency. In addition, it should also include some requirements to ensure the operating rules for trading platforms on crypto-assets are transparent and readily available to the public.

109. The second dimension relates to the level of data disaggregation that trading platforms are required to make available to users.

## 4.2 Assessment

### 4.2.1 Transparency

#### Background

110. MiCA establishes a regulatory framework aimed at ensuring transparency in the operations of trading platforms for crypto-assets. Article 76 underscores the necessity for these platforms, operated by CASPs, to maintain clear and transparent operating rules, and to disclose pre-trade and post-trade data to the public. This includes detailed information about bid and ask prices, the depth of trading interests, and the specifics of executed transactions. The intent is to bring the transparency standards of crypto-assets closer to those of traditional financial instruments, fostering a more secure and reliable trading environment for all market participants.

#### Feedback to the consultation

111. Feedback received has been broadly supportive of ESMA's proposed approach to further define how transparency data is to be presented and aligning it to the extent possible with standards applicable on traditional markets. Nonetheless, stakeholders have expressed some concerns about the challenges associated with the practical implementation of these measures, emphasising that implementing and maintaining the proposed transparency measures will necessitate sophisticated technological solutions, leading to associated compliance costs. In addition, stakeholders also emphasised the need for clarity in defining the operational scope of centralised exchanges (CEXs) and decentralised exchanges (DEXs), and how transparency requirements apply to each. The feedback underscored suggestions including refining the definitions of CEXs and DEXs, acknowledging the emergence of hybrid models, and making operating rules readily accessible to the public.

#### ESMA assessment and recommendations

112. In response to the feedback and in light of the significant support received to the proposals in the CP, ESMA has decided not to make any substantial changes to the proposal in the draft RTS. However, ESMA added a recital to the RTS to introduce a description of CEXs and provide further clarification on the scope of DEXs in light of recital 22. ESMA notes that the exemption of Recital 22 is only provided for services that

are provided in a “fully decentralised manner without any intermediary”. Considering the restrictive nature of this exemption, it was decided that the draft RTS should also include transparency obligations for those DEXs which are not exempt from MiCA pursuant to Recital 22.

## 4.2.2 Pre-trade transparency

### *Description of trading systems*

#### **Background**

113. Table 1 of Annex I of the draft RTS describes the pre-trade transparency requirements for each type of trading system commonly employed by crypto-asset trading platforms, including continuous auction order books, as well as quote-driven, periodic auction, automated market makers (AMMs), and hybrid systems. With the exception of AMMs, the other trading systems in the table mirror those listed in Annex I of Commission Delegated Regulation (EU) 2017/587 (MiFIR RTS)<sup>9</sup>.
114. In the CP, ESMA asked stakeholders to confirm this list of trading systems and provide examples of other types that may be used by trading platforms in crypto-asset markets. The objective of this section of the consultation was also to discover what (if any) pre-trade transparency elements could have been added to the draft RTS.

#### **Feedback to the consultation**

115. Most respondents considered the types of trading systems listed in Table 1 of Annex 1 of the draft RTS sufficient to capture the range of systems used in crypto-asset trading (with endorsement for the ‘other’ category as a catch-all). Respondents noted that they currently use at least one type of system listed, with the most commonly cited being the continuous auction or central limit order book (CLOB). In addition, several respondents noted that they already make available basic elements of pre-trade information to the public, including the aggregated numbers of orders and the amount of crypto-assets they represent at each price level for more than the five Best Bid And Offer price (BBO) levels.
116. One respondent voiced concern that the MiFIR principles for trading systems (upon which the annex table was based) may not be fit for purpose for crypto-asset markets. To illustrate this, the respondent used the hypothetical case of an auction of a tokenised real-world asset in which pre-trade transparency would not technically be possible. ESMA would stress that such assets, including NFTs, would only enter into the scope of MiCA (and hence subject to trade transparency obligations in Article 76(9)) if they qualify as crypto-assets.
117. A respondent with an interest in the prevention of market abuse proposed that ESMA establishes requirements for operators of CLOB trading systems to make their entire

---

<sup>9</sup> OJ L 87, 31.3.2017, p. 387–410 ([link](#))



order book public (instead of ‘at least’ the five BBO). This same respondent also asked for clarity on the MiCA’s treatment of Matched Principal Trading (MPT) and whether entities engaged in MPT would be considered trading platforms for crypto-assets even if this same entity does not offer an order book (or any of the other listed trading systems). Finally, this respondent argued that liquidity provision in an AMM context should be equated to ‘dealing on own account’ which they argued is not covered by the MiCA regime.

118. Another respondent with knowledge of AMMs proposed an extension (or modification) of the text in Table 1, including the addition of qualifying language to clarify that AMM systems would only be in scope of MiCA when operated by a CASP. The same respondent also proposed a revision to the description of AMMs in the table (further specifying how price formation occurs in a liquidity pool) and how pre-trade information should be made public when such systems are used. This description in the Annex, another respondent said, should be mirrored in Recital 5 of the draft RTS.
119. For AMMs, several respondents cited ‘price slippage’<sup>10</sup> as an important indicator of the riskiness of the liquidity pool as well as ‘swap fees’<sup>11</sup> and the balances of each crypto-asset in the pool. Another comment from respondents focused on the share of liquidity in the pool held by individual wallets. For users of an AMM trading system, or for depositors in the pool, this information may allow them to make more informed decisions about how and where to transact.

### **ESMA assessment and recommendations**

120. Based on feedback to the description of AMMs in Table 1 of Annex 1 and the associated information to be included in pre-trade transparency, ESMA has added details to row no. 4 about ‘liquidity in the pool at any given moment’ to complement the mathematical equation (see box below). Although some respondents requested additional details about smart-contract platforms and permissioned vs. permissionless protocols, ESMA has elected not to incorporate this because it is immaterial to the type of trading system. On this same subject, however, ESMA confirms the views of those respondents citing Recital 22 to say that those AMMs operated in a “fully decentralised manner without any intermediary” should be outside the scope of this RTS

---

<sup>10</sup> Price slippage refers to the change in price after execution of a trade caused by exogenous market movements (unrelated to a user’s trade) or caused by the user’s own trade (this latter concept is also often referred to as ‘price impact’)

<sup>11</sup> Fees paid to liquidity providers as remuneration for lending their crypto-assets to the liquidity pool. Not to be confused with ‘gas fees’ which are paid to the node(s) validating the transaction as a reward for consensus (and therefore not a function of the AMM itself)

**Proposed changes to Table 1, Annex I of the draft RTS**

1) Amendment to **‘Automated Market Maker’ (#4) / Column:** Description of the trading system

~~“A decentralised protocol relying on liquidity pools and smart contracts which allows the execution of individual transactions in a permissionless and automatic way.”~~

**“A system relying on liquidity pools and mathematical pricing and valuation models for the automatic execution of individual transactions.”**

--

2) Amendment to **‘Automated Market Maker’ (row 4) / Column:** Information to be made public

*“(i) the mathematical equation used to determine the price at which assets can be exchanged;*

***(ii) the level of liquidity in the liquidity pool at a given moment in time (on a continuous basis); and***

*(iii) any further information or parameters that allow for the determination of the price at which a specific order would be executed.’*

121. Several respondents mentioned ‘price slippage’ or ‘price impact’ as an element to include for pre-trade transparency for AMMs. Indeed, many AMMs already allow users to choose a slippage range (or ‘tolerance’) for their bids and offers and provide alerts when the trade would fall outside the normal fluctuations of the pair exchange rate (in situations of low liquidity). Although ESMA considers pre-trade information on price impact useful, it is not made mandatory in the RTS. However, CASP trading platforms are encouraged to provide such information, which would fall into the category of ‘any further information’ (in 2(iii) in the box above), where necessary and on a voluntary basis.
122. Another suggestion from respondents was to require transparency around the proportions of liquidity pool shares held by individual wallets (i.e., how is liquidity in the pool concentrated among the liquidity providers). Implementing transparency around the concentration of pool shares would be possible in the case of a CASP operated AMM because of the know-your-customer (KYC) obligations under Article 76(1)(a) of MiCA. Imposing KYC on liquidity providers would sidestep the problem of default pseudonymity in the use of self-custody wallets, which in other contexts (decentralised protocols) would allow liquidity providers to obscure the actual proportions of the crypto-asset pair they hold in the pool. However, ESMA does not see any added value for users of the platform in requiring CASPs to publish this data for pre-trade transparency purposes.
123. As for the treatment of MPT, this is addressed in Article 76(6) of MiCA, which allows trading platforms for crypto-assets to provide such intermediation when clients have, ‘consented to that process’ and where it ‘does not give rise to conflicts of interest between the crypto-asset service providers and their clients’. This article however is not part of

the mandate under Article 76(16)(a). ESMA will reflect whether the boundaries of engaging in MPT and the operation of a trading platform require further guidance outside of the remit of this final report.

### *Pre-trade transparency information*

#### **Background**

124. The CP noted that while the general description of the information to be provided for the purpose of pre-trade transparency per trading system already improves the pre-trade information disclosed, ESMA considered it necessary to further align the practices for disclosing pre-trade information. To that effect, ESMA proposed to complement the information described in Annex I of the draft RTS by inserting a table establishing clearer obligations regarding the specific information which is expected to be published for each order and provide for a harmonised content and format.
125. ESMA requested feedback on whether respondents agreed with the proposals on the description of the pre-trade information to be disclosed and to require a specific format to standardise the information to be disclosed.

#### **Feedback to the consultation**

126. All (but one) respondent that provided a view on the proposal to standardise the information to be provided agreed with ESMA. In addition, the majority of respondents also agreed with ESMA's proposal to standardise the pre-trade information to be disclosed. Nevertheless, some of these respondents noted that this may lead to higher compliance costs to implement the proposed format.

#### **ESMA assessment and recommendations**

127. In light of the significant support received to the proposals in the CP, ESMA will keep the pre-trade information to be made public on Tables 2 and 3 Annex I unchanged, apart from some minor changes introduced to ensure consistency with other Level 2 mandates under MiCA.

### *Reserve and stop orders*

#### **Background**

128. The CP also looked at specific type of orders offered by trading platforms and suggested a way forward on how pre-trade transparency would apply to those. In particular, ESMA understands that trading platforms on crypto-assets offer a variety of order functionalities or types, order book limit or good 'til cancelled orders being the most common, especially in the context of CEXs. In the CP, ESMA expressed its view that orders that meet the conditions defined in the draft RTS can be offered by trading platforms.

129. The CP therefore considered that some orders, such as (i) reserve orders and (ii) other orders, e.g. stop-loss orders or one-cancels-the-other orders should still be allowed under MiCA. ESMA considered it important to ensure that trading platforms can offer these order features to their clients considering in particular the very large proportion of retail investors. Such investors would otherwise not have access to these risk management tools which would put them at a considerable competitive disadvantage with institutional investors who will anyhow be able to use similar features through external order management facilities.
130. Therefore, ESMA proposed in the CP to calibrate the pre-trade transparency regime for crypto-assets so that orders which meet three conditions, can be offered by trading platforms under the MiCA framework and be considered to meet the transparency obligation by being published, in accordance with the details under Table 1 of Annex I of the draft RTS, only once released into the order book. The conditions set forth in the draft RTS were:
- i. the order is intended to be disclosed to the order book operated by the trading venue and is contingent on objective conditions that are pre-defined by the system's protocol;
  - ii. the order cannot interact with other trading interests prior to disclosure to the order book operated by the trading venue;
  - iii. once disclosed to the order book, the order interacts with other orders in accordance with the rules applicable to orders of that kind at the time of disclosure.

### **Feedback to the consultation**

131. All respondents agreed with ESMA's proposed approach to reserve and stop orders. However, some respondents considered that, although noting the legislative constraints, ESMA should consider other exemptions to pre-trade transparency. In particular, these respondents consider that waivers for large orders are crucial for crypto markets.

### **ESMA assessment and recommendations**

132. In light of the significant support received to the proposals in the CP, ESMA will not make any changes to the proposal in the draft RTS.
133. ESMA acknowledges the feedback received from some stakeholders that some exemptions to pre-trade should be considered. However, ESMA would like to reiterate that MiCA does not include any pre-trade transparency waivers and that ESMA cannot create an exemption in the RTS, for example for large orders, as it is outside the scope of the Article 76(16)(a) mandate.

### **4.2.3 Post-trade transparency**

## *Post-trade transparency information*

### **Background**

134. Like MiFIR (Articles 6 and 10), MiCA (Article 76(10)) also sets out post-trade transparency requirements for CASPs operating a trading platform in crypto-assets to make public the price, volume and time of the transactions executed.
135. In the CP, ESMA proposed to set out in the draft RTS the appropriate data fields that have to be included by crypto-asset trading platforms when publishing post-trade information.

### **Feedback to the consultation**

136. Three questions were asked in the context of post-trade transparency namely, if they agreed with the list of fields proposed, if they considered such fields sufficient to identify the traded contract and to compare the reports to the same / similar contracts and, if they would consider it necessary to add any additional field. In general stakeholders agreed with the first two questions. However, some remarks were made.
137. More specifically, a respondent suggested that information on fees or any other costs associated with the transaction could be relevant. The same respondent also proposed disclosing the Financial Instrument Global Identifier (FIGI) as well as information related to the blockchain network (like block confirmation numbers), as this might, according to this respondent, enhance the quality of post-trade information. It is considered that some of those information could be included in the transaction identification code (field 12). Therefore, no additional field is added.
138. Furthermore, on one hand it was considered that the "crypto-asset full name" field was not necessary since the information of the crypto-asset admitted to trading would be completed with the "Crypto-asset identification code" field (field 3). On the other hand, it was recommended to specify the stabilisation mechanism of a crypto-asset, in particular for Asset-Referenced Tokens ("[...] referencing another value or right or a combination thereof, including one or more official currencies") and to include any information with regard to the type / nature of crypto-asset traded. This information is included in the crypto asset identification code (field 3) and in the crypto asset full name (field 4) and it is deemed to be relevant to include both to make sure that all information related to the currencies backing the crypto asset are identified. Therefore, no additional field has been added.
139. Finally, a proposal was made to include the order-type in the post-trade transparency disclosure, i.e. limit orders, stop-limit orders, market orders, fill-or-kill etc. The argument from respondents is that, since large market orders are often executed at various prices as they fill the other side of the CLOB, the trader should be made aware of both the average price of his trade (encompassing all of the sub-transaction executions) and the percentage/quantity of his transaction filled at each price after execution. However,

ESMA considers that this information should be considered as pre-trade data and, sensitive information for traders that would exponentially increase the level of information to be made public. Furthermore, the inclusion of this information would create confusion on the type of information which is published. Consequently, it was not considered appropriate to add these fields to the post-trade transparency reports.

140. Finally, it was indicated that for the initial quantity (Field 25 of Table 2 Annex II) the standard allowing for a maximum number of 18 digits of which a maximum of 17 fraction digits may be insufficient and incur a loss of information, since many assets support a large number of fraction digits - 18 in the case of Ethereum.
141. In addition to the feedback sought on the information that trading platforms have to publish, the CP also requested stakeholders' views on whether the required data fields would be difficult to obtain.
142. Overall, respondents did not foresee any particular challenges for trading platforms in crypto-assets to obtain the data fields required for the publication of pre-trade and post-trade transparency data. However, some respondents noted that appropriate implementation time should be given for trading platforms to have systems in place to comply with their obligations. In addition, they further noted that they would incur potential implementation costs.

### **ESMA assessment and recommendations**

143. In conclusion, on the basis of the feedback received, ESMA has decided only to amend some fields to ensure consistency with other Level 2 mandates under MiCA.

### *Real-time publication*

#### **Background**

144. In the context of traditional equity instruments under MiFIR, trading venues are required to publish post-trade information as close to real-time as is technically possible and in any case within one minute after execution. For non-equity instruments, the time is increased to within five minutes after execution.
145. Despite the time lags allowed in the other sectoral Regulations, ESMA considered in the CP that post-trade transparency data in relation to crypto-asset transactions could in most cases be published immediately after execution. Nevertheless, ESMA proposed in the CP to still allow for some leeway for trading platforms but considered reducing the maximum time limit set for financial instruments, in particular the requirement set for equity instruments. ESMA therefore proposed that trading platforms in crypto-assets make post-trade information available to the public as close to real time as is technically possible and in any case within 30 seconds of the relevant transaction.

#### **Feedback to the consultation**



146. Respondents considered different maximum delays in order to fall under the definition of “as close real-time as is technically possible”, with some respondents making proposals ranging from as long as two hours to 15 or 10 minutes.
147. Nevertheless, it should be noted that the vast majority of respondents, despite agreeing that a transaction on a CEX could be published very quickly (i.e. below the 30 seconds proposed by ESMA), considered that the requirements applicable to crypto-assets should be aligned with traditional instruments (shares in particular) and a one-minute delay should be allowed for cryptos.
148. Respondents noted that there may be circumstances, for example due to adverse market conditions or the underlying technology, that justify the alignment with the requirements under MiFIR for traditional assets.
149. One respondent was also concerned that the current regime does not allow for a specific delay for large block trades (unlike the CFTC). They urge ESMA to consider allowing for delays depending on the type or size of the transaction. For DEX, the feedback was clear that the time needed is longer than for off-chain transactions given their characteristics. However, only one respondent suggested a timeframe – 24 hours – whilst the majority noted that the timeframe to publish on-chain transactions can vary and the availability of information may not be consistent.

### **ESMA assessment and recommendations**

150. ESMA noted the feedback received from stakeholders noting that in a CEX context, transactions can be published below the 30 second requirement proposed by ESMA. Nevertheless, ESMA also understands respondents’ suggestion to align the requirements with traditional instruments, in particular equity instruments. Nevertheless, it should be noted that also for traditional exchanges and trading platforms, in particular order book trading, ESMA is considering reducing the timespan required to publish a transaction in the context of the MiFIR review.
151. Therefore, considering the technological developments in the markets and the ability, confirmed by the responses received, of trading platforms to publish within 30 seconds, ESMA retained its initial proposal. As a consequence, trading platforms in crypto-assets should make post-trade information available to the public as close to real time as is technically possible and in any case within 30 seconds of the relevant transaction.
152. It should be taken into consideration also that ESMA expects transactions to be published immediately after execution in accordance with the technology used by the trading platform and that the maximum 30 seconds delay should only be used in justified cases. It should be noted that no artificial delays should be introduced to delay the publication of transactions.
153. ESMA also reiterates the indication already described in the CP that the post-trade requirements for crypto-asset platforms apply when the transaction is agreed on the

trading platform which may not coincide with when it is eventually reflected on the blockchain. In particular in the case of CEX, ESMA understands that not all transactions are systematically registered immediately on the blockchain, exchanges for instance updating the DLT records at a predefined frequency.

#### 4.2.4 Operating conditions

##### Background

154. In establishing a regulatory framework for crypto-assets under MiCA, a critical focus has been placed on the operating conditions for trading platforms. These conditions are fundamental in ensuring transparency, fairness, and integrity within crypto-asset markets. The operating rules set forth by CASPs aim to facilitate a clear understanding of the trading environment for all participants, aligning with the standards observed in traditional financial markets. The discourse around these rules has touched upon various aspects, including but not limited to, co-location, access arrangements, and the dynamic nature of trading conditions.

##### Feedback to consultation

155. Stakeholders have predominantly supported ESMA's proposed approach towards trading platforms' operating conditions, appreciating the balance sought between comprehensive disclosure and operational flexibility. Feedback highlighted a consensus against imposing overly specific disclosure requirements, particularly concerning co-location and access arrangements. This reflects a preference for maintaining a level of adaptability within the regulatory framework to accommodate the unique and evolving nature of crypto-asset markets.

156. Furthermore, suggestions were made regarding the consolidation of operating rules into a single document to enhance accessibility and comprehension for users, alongside the potential for dynamic web updates to address the fluidity of trading conditions.

##### ESMA assessment and recommendations

157. Given the feedback and the supportive stance from stakeholders towards the draft RTS's approach to operating conditions, ESMA proposes to proceed as outlined in the CP, without incorporating more specific disclosure rules related to co-location and access arrangements.

158. However, recognising the value in stakeholders' suggestions, ESMA agreed to incorporate the importance of presenting operating rules in a singular, comprehensive document by amending Article 3(1) of the RTS<sup>12</sup>. This approach is designed to simplify

---

<sup>12</sup> Art. 3(1) amended, "Crypto-asset service providers shall provide the information required by this Regulation free of charge, in a downloadable file, in a way that is easy to read, using characters of readable size and using a style of writing that facilitates its understanding. **Crypto-asset service providers operating a trading platform for crypto-assets shall consolidate all operating rules and related policies into a single comprehensive document.**"



access to critical information for issuers and investors, promoting a deeper understanding of the trading platform's operating environment.

#### 4.2.5 Data disaggregation

##### Background

159. Under Article 76(11), MiCA requires trading platforms for crypto-assets to make pre- and post-trade data available on a reasonable commercial basis and accessible on a non-discriminatory basis. MiCA also requires trading platforms to make this data available free of charge after 15 minutes and to remain published for two years. The draft RTS specifies the minimum level of disaggregation that should be offered by trading platforms when making this data available.
160. In the CP, ESMA asked stakeholders if they supported the level of disaggregation specified in Article 5 (and indirectly, Recital 7) of the draft RTS. Specifically, ESMA proposed in the draft RTS to require trading platforms for crypto-assets to offer their disaggregated transparency data upon request in intervals or bundles so end-users or clients can tailor the purchases of that data to their specific needs while meeting the 'reasonable commercial basis' and 'non-discriminatory access' standards in Article 76(11).

##### Feedback to the consultation

161. Most respondents supported the proposal, confirming that the level of disaggregation proposed in Article 5 of the draft RTS is sufficient to meet transparency requirements. There was also broad support for disaggregation on a crypto-asset basis when available.
162. Several respondents called for additional clarity around the concept of data being available for 'minimum periods of one week' per Article 5(3) of the draft RTS (and 'access to historic series on a per-week basis' in Recital 7). The consensus view is that this parameter may not be feasible to provide for regular or heavy users of the trading platform (for cost reasons). Here the respondents noted the important distinction between users of the trading platform for trading activities and those who collect (or buy) the data for further aggregation and value-added services.
163. In response to a general question about (default) availability of data in the crypto-asset industry, respondents said that many trading platforms for crypto-assets already offer certain types of disaggregated market data freely at present (either through APIs or real-time order books on their trading interfaces). Data is typically available for prices on crypto-to-crypto or crypto-to-fiat pairs. Responses varied in terms of the granularity, time to publication, and the intervals or starting dates for historical time series. Although today this market data tends to be free, according to respondents (on a limited basis, i.e. a fixed number of API queries per day/minute), it will likely become a source of revenue for trading platforms for crypto-asset in the future as competitive pressures increase. Indeed, one respondent said some trading platforms for crypto-assets currently charge

a fee to access more sophisticated types of market data on a more disaggregated basis. Here, the price may depend on the profile of the data user: professional or retail.

### **ESMA assessment and recommendations**

164. Based on the consultation feedback, ESMA proposes removing paragraph 3 from Article 5 of the draft RTS (and the associated text in Recital 7). Although a majority of respondents supported the level of granularity for disaggregated data to be made available to the public, providing real-time data in bundled time series of weekly intervals was not considered feasible.
165. MiCA requires CASP trading platforms to make pre-and-post-trade transparency data 'available to the public on a reasonable commercial basis' – therefore it is implied that trading platforms for crypto-asset may monetise their real-time data. However, this monetisation can only happen before it is made available freely 15 minutes after publication. Such data would remain published for at least two years which means end-users or clients would be able to tailor their preferred time series or intervals within that timeframe.

## 5 Record keeping obligations for CASPs

### 5.1 Background and legal basis

#### Article 68(9) and (10) of MiCA

*“9. Crypto-asset service providers shall arrange for records to be kept of all crypto-asset services, activities, orders, and transactions undertaken by them. Those records shall be sufficient to enable competent authorities **to fulfil their supervisory tasks and to perform enforcement measures**, and in particular to ascertain whether crypto-asset service providers have complied with all obligations including those with respect to clients or prospective clients and to **the integrity of the market**.*

*The records kept pursuant to the first subparagraph shall be provided to clients upon request and shall be kept for a period of five years and, where requested by the competent authority before five years have elapsed, for a period of up to seven years.*

*10. ESMA shall develop draft regulatory technical standards to further specify:*

*(a) the measures ensuring continuity and regularity in the performance of the crypto-asset services referred to in paragraph 7 [mandate covered in Section 3]*

*(b) the records to be kept of all crypto-asset services, activities, orders and transactions undertaken referred to in paragraph 9. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010.”*

166. Article 68 of MiCA sets forth the organisational requirements for CASPs. These include the obligation to keep records of all crypto-asset services, activities, orders and transactions undertaken by them, and provide such records to competent authorities and clients upon request. ESMA is mandated to further specify what records shall be kept.

167. The records to be kept under Article 68(9) of MiCA shall “be sufficient to enable competent authorities to fulfil their supervisory tasks and to perform enforcement measures, and in particular to ascertain whether crypto-asset service providers have complied with all obligations including those with respect to clients or prospective clients and to the integrity of the market”. Since consistency and comparability of data is essential for competent authorities to seamlessly perform the analysis across datasets, and to exchange supervisory information with other competent authorities, CASPs should provide records of orders and transactions to competent authorities in a standardised form, both in terms of content and format.

### **Article 76 (15) and (16) of MiCA**

*“15. Crypto-asset service providers operating a trading platform shall keep at the disposal of the competent authority, for at least five years, the relevant data relating to all orders in crypto-assets that are advertised through their systems, or give the competent authority access to the order book so that the competent authority is able to monitor the trading activity. That relevant data shall contain the characteristics of the order, including those that link an order with the executed transactions that stem from that order.*

*16. ESMA shall develop draft regulatory technical standards to further specify:*

*(a) the manner in which transparency data, including the level of disaggregation of the data to be made available to the public as referred to in paragraphs 1, 9 and 10, is to be presented;*  
[mandate covered in Section 4]

*(b) the content and format of order book records to be maintained as specified in paragraph 15.”*

168. Article 76 of MiCA lays down the operational requirements for CASPs operating trading platforms for crypto-assets. Paragraph 16 of that Article sets the obligation to keep records of all orders in crypto-assets that are advertised through their systems and to make such records available to the regulators or provide access to the order book. ESMA is mandated to further specify the content and format in which those order book records shall be kept.

169. With respect to order data to be kept by CASPs operating trading platforms, the empowerment in Article 76(16) expressly mandates ESMA to develop draft RTS to specify both content and format of the “relevant data relating to all orders in crypto-assets that are advertised *through their systems*”. It also further defines this dataset as including the “*characteristics of the order, including those that link an order with the executed transactions that stem from that order*”.

## **5.2 Assessment**

### **5.2.1. On-chain specific data elements**

#### *Identification of crypto-assets and transactions*

##### **Background**

170. ESMA analysed the option of adding on-chain specific data elements that should be included in records of both CASPs and CASPs operating a trading platform. As stated in the Consultation Paper, it is necessary to uniquely identify a specific crypto-asset to enable competent authorities to effectively monitor its trading activity. To identify the crypto-asset, ESMA proposed using the Digital Token Identifier (DTI), which can be used as well for reporting the price and quantity of the transactions in the case of transactions

priced in crypto-assets, which are not covered by the traditional ISO currency classifications. The DTI is issued and maintained by the DTI Foundation (DTIF). Additionally, the DTIF also maintains certain technologically relevant information related to each DTI, which can be accessed and downloaded from the DTIF register.

171. In the Consultation Paper, ESMA asked the stakeholders if they agree with using the DTI for uniquely identifying the crypto-assets for which the order is placed, or the transaction is executed, as well as for reporting the quantity and price of transactions denominated in crypto-assets. In addition to the DTI, stakeholders were asked if there are any relevant technical attributes describing the characteristics of the crypto-asset or of the DLT on which this is traded, other than those retrievable from the DTIF register.
172. Lastly, the Consultation Paper explored whether the transaction hash could be used to uniquely identify the transactions that are fully or partially executed on-chain in orders and transaction records. The transaction hash is already available since it is automatically generated on the DLT and therefore removes the burden for trading platforms to generate and maintain an additional trade identifier. In the Consultation Paper, the stakeholders were asked if they agree with using the transaction hash to uniquely identify transactions that are fully or partially executed on-chain in orders and transactions records.

### **Feedback to the consultation**

173. A large majority of respondents supported the proposal of using DTI to uniquely identify crypto-assets for which the order is placed or the transaction is executed and for reporting the quantity and price of transactions denominated in crypto-assets, either outright or with some comments. Seven respondents supported the proposal to use the DTI for both purposes outright. Only four respondents disagreed with the proposal made. A few respondents primarily expressed concerns regarding the adoption level of the DTI not being broad enough and suggested the exploration of alternative identifiers and standards for crypto-asset identification, such as FIGI, ISIN or ITIN<sup>13</sup>, and token addresses/contracts. Alongside these concerns, governance and geographical issues were highlighted. Respondents also proposed technical adjustments, such as increasing character limits in certain data fields. The potential cost and burden on smaller players were also highlighted.
174. With regards to the technical attributes retrievable through the DTIF register, four respondents considered them to be sufficient in order to describe the characteristics of the crypto-asset or of the DLT on which it is traded. Additional attributes deemed as relevant by respondents were token definition contract for secondary tokens defined through smart contracts (three respondent), the token standard (two respondents), references to other identifiers (one respondent), tokenomics (one respondent),

---

<sup>13</sup> The International Token Identification Number (ITIN) is developed by the International Token Standardization Association (<https://my.itsa.global/>). It is not an ISO standard.

environmental impact (one respondent), information on a standardized rounding of asset quantities (one respondent), hashing power for Proof of Work Coins (one respondent), and issuers' ID or LEI (one respondent).

175. As for the transaction hash, 11 respondents agreed to proceed with ESMA's proposal of using the transaction hash as a unique identifier for fully or partially executed on-chain in orders and transactions records as long as the integrity of the transaction is guaranteed. A couple of respondents, while not disagreeing with its use, suggested that it might not be in all cases identifying these uniquely since multiple trades can be settled in one transaction. One respondent clarified that transaction hashes could potentially represent a multitude of actual transactions possibly relevant for multiple users, putting in question their usefulness as unique identifiers for these transactions. Respondents generally fully supported ESMA's view that any additional means of identification would present an unnecessary burden to trading platforms when an on-chain transaction is performed.
176. Lastly, for situations where hybrid systems are used, several respondents supported the use of the transaction hash as the best means to uniquely identify transactions all while warning of its limitations in these cases. One respondent considered less clear whether hybrid systems would need a more nuanced approach to ensure that transactions are accurately and reliably identified regardless of whether they are executed on-chain, off-chain, or through a combination of both. Another respondent suggested adding a field for "linked transaction" to address this.

### **ESMA assessment and recommendation**

177. A strong majority of the respondents, 16 out of 20, supported the use of DTI. Among the criticisms made of the use of DTI, the most prevalent were the location outside of the EU of the DTI Foundation, costs which would be unfair to smaller market players, and the existence of other identifiers (i.e., ISIN/ITIN/FIGI or other).
178. Regarding the location of the DTI Foundation, the DTI Foundation is indeed headquartered in the United Kingdom, however, it has recently opened an office within the EU located in Amsterdam. Furthermore, many international standards' organisations are located out of the EU with no prejudice to their ability to set standards. The International Organization for Standardization (ISO) is one such case which is located in Switzerland. Secondly, with regards to the costs, the DTIF has indicated that it will pursue a cost model based on a cost recovery basis comparable to the existing models of the ISIN or UPI with ANNA-DSB. Finally, when comparing the DTI with other identifiers, it has been determined as the most suited to identify crypto assets for the purpose of MiCA. Indeed, using identifiers already mandated for the identification of financial instruments (such as the ISIN) would inaccurately conflate crypto assets with financial instruments. In addition, at present, the ISIN cannot be assigned to the full population of crypto-assets that are not financial instruments and is not granular enough as it identifies crypto assets at the asset level (rather than at the token level).

179. The FIGI standard, mentioned by one respondent was also considered. However, the FIGI is not a sufficient identifier as it also not granular enough, identifying crypto assets at the asset level, and the information needed for identification of crypto assets in the context of transaction data is not available for free. The concomitant use of two identifiers (FIGI and DTI) would increase the burden on investors, CASPs, and regulators and as such, is not a viable option. Furthermore, the DTI presents the advantage of being directly linked to the ISIN standard, already mandated under other reporting regimes, at the level of the Functionally Fungible Group. Other identifiers, such as the token address or contract, are less suitable than the DTI for the purpose of uniquely identifying crypto assets as they are not standardized across different blockchains and are not defined as ISO standards.
180. In light of the feedback received and the strong majority of respondents supporting the use of the DTI standard to identify crypto-assets, ESMA will maintain the proposal in the Consultation Paper to mandate the DTI to identify crypto-assets in orders and transactions, as well as to report the quantity and price of transactions denominated in crypto-assets. However, the text in the technical standards leaves the door open to alternative identifiers should any alternative be deemed in the future as fulfilling the set of criteria deemed necessary for a robust identification system. At present, the market supervisors are not aware of any other alternative identifier that would fulfil the same criteria.
181. Regarding the technical attributes, there was no clear majority in favour of any specific characteristic describing crypto-assets or describing the DLT on which crypto-assets are traded in the consultation responses. Rather, respondents listed multiple attributes they deemed as useful. ESMA will communicate these attributes to the DTI maintenance agency, the DTI Foundation, while also highlighting the feedback that too many attributes and attributes that are too complex might have adverse effects for retail investors. Indeed, in its response, the DTI Foundation highlighted that it “welcomes feedback on any other potential relevant technical attributes which could be added to the DTI Registry to support wider implementation of the ISO 24165 standard”.
182. Lastly, given the broad support by respondents ESMA suggests proceeding with its original proposal of using the transaction hash for the identification of transactions that are partially or fully executed on-chain in order and transaction records, including transactions undertaken with hybrid systems. While the specific name of the field could be changed to account for different technologies, “transaction hash” is not only the immediately recognizable term, but also the one that leads to less confusion than the artificial creation of a new term.

### *Additional data elements specific for on-chain transactions*

#### **Background**



183. As mentioned in the Consultation Paper, by leveraging on the results from the independent study by PwC<sup>14</sup> related to the DLT Pilot Regime, ESMA proposed to add additional data fields related to on-chain trading for both RTSs. Therefore, in the Consultation Paper, ESMA asked the stakeholders on their views on the inclusion of the proposed on-chain data elements, whether any other data elements should be considered as well or if the data elements are technology-specific (i.e. not relevant or applicable to other DLTs). Among these fields relating to on-chain trading it was proposed to have a separate field for the recording of “gas fees” with the purpose of identifying the sequencing of orders and events affecting the order. Finally, it was also asked if the stakeholders consider it necessary to add a different timing for the provision of identification codes for orders in the case of CASPs operating a platform which uses only on-chain trading.

### **Feedback to the consultation**

184. While a plurality of respondents agreed with the usefulness of providing a field to register “gas fees” for on-chain transactions, many did not believe this to be absolutely necessary or a priority for the purposes of these TS. Some respondents questioned this field’s usefulness when determining the sequencing or prioritization of orders due to the way gas fees are structured and combined with other fees. Other respondents did see the usefulness to include them for even additional purposes, such as identifying trading patterns like high-frequency trading or activities of market makers. Some respondents questioned their usefulness for trades involving hybrid systems. One respondent signalled the fact that this term is commonly used to refer to Ethereum fees and suggested keeping the approach technology-neutral, suggesting the use of the name “transaction fees” while another respondent suggested the more general name of “network fees”. Some respondents mentioned the fact that other fields in these RTS (i.e., transaction hash, timestamp) could help achieve the same goals without including a field for “gas fees”. Other respondents suggested that ESMA should further clarify the specific cases for which it intends to use this information and suggests this field to be made voluntary.<sup>185</sup> As for the rest of data fields specific for on-chain transactions, the vast majority of respondents supported their inclusion, with wide support to the inclusion of a specific on-chain trading data table. Some respondents however, signalled that creating a custom standard may impede its applicability to all digital asset technologies. Certain respondents made reference to suggestions to other fields previously discussed in this report and which have already been addressed. One respondent asked for clarifications with regards to data privacy issues and asked for reassurance in case the information cannot be retrieved from unhosted wallets. With a few exceptions who confirmed their universality, albeit with different names, and as explained in the previous section, almost all respondents identified gas fees, gas limits and certain as well identified data size and smart contracts as specific to certain technologies, most commonly Ethereum. Respondents suggested to adapt these requirements to be more flexible to the different

---

<sup>14</sup> [ESMA12-2121844265-3183 Report on the DLT Pilot Regime - Study on transaction reporting based on RTS 22 \(europa.eu\)](#)

technologies, while reminding the different technologies and their similarities and differences when it comes to achieving the objectives those fields were set up to.

186. Furthermore, several respondents suggested or supported the inclusion of certain additional data fields to properly account for on chain trading specificities. There were some respondents supporting ESMA's inclusion of hash or combining it with the HMAC or other pointers to identify data stored in off chain databases. Other respondents suggested the inclusion of Method ID to allow for the provision of details on the type of transaction and the function call for ERC20 tokens. However, there were again mentions to avoiding technology specific terms (such as Method ID) or "gas fees". It was also suggested to add separate fields for an identifier like "vout" or "vout output" and trade execution date.
187. Lastly, a majority of respondents agrees that CASPs operating a platform that uses only on chain trading should be allowed to have a different timing for the provision of identification of orders due to the unique characteristics of the blockchain technology and the time it needs for the processing of the transaction, block creation and confirmation as well as congestion of the networks and settlement timing. One respondent disagreed by stating that the fact that transactions can be given immediate identifiers is proof that orders can do so equally. The respondent notes there are several technological solutions available to ensure this. Finally, one respondent supported keeping the distinction while making certain remarks on the timing of the provision of the information that seem to concern more transaction information rather than only one relating to orders.

### **ESMA assessment and recommendation**

188. Regarding the "gas fee", generally respondents have widely recognized the different uses of recording the "gas fees" as a separate field that would help identify the priority and cost requirements associated with a transaction. Because of this, ESMA suggests keeping its initial proposal of keeping a separate field for these fees. There have been however, several respondents clarifying that these apply mostly only to transactions happening on chain as well as in hybrid systems. ESMA therefore suggests including it as a mandatory field only for on-chain trading. Finally, respondents generally reminded ESMA that the specific terms "gas fees" is mostly applied only to Ethereum and therefore ESMA suggests naming the field "network fees", as this term seem to be widely used and not associated with either Ethereum or Bitcoin as the other suggested terms.
189. Given the broad support of its proposal, ESMA suggests maintaining its initial proposal with regards to fields specific to on-chain transactions, notwithstanding the changes mentioned in other questions to this consultation, including those related to changes in the name of certain fields to reflect a technology-neutral approach.
190. Lastly, given the broad support for providing a different time for the provision of identification codes for orders in the case of CASPs operating a platform using only on-chain trading, ESMA suggest proceeding with the proposed approach.

## 5.2.2. Data elements to be included in the records of all CASPs

### *Definitions in the draft RTS*

#### **Background**

191. Pursuant to Article 68(9) of MiCA, the obligation to keep records of “*services, activities, orders and transactions*” applies every time one of those is “*undertaken*” by the CASP. However, the expression of “undertaking” a transaction is neither defined in MiCA nor has an equivalent in the terminology used in the MiFIR data reporting technical standards or in other pieces of EU financial legislation, Therefore, ESMA tried to define the terms “transaction”, “undertaking a transaction” and “executing a transaction” in the RTS.
192. In the Consultation Paper, ESMA asked stakeholder if the defined terms were clear enough and if there are any other aspects that should be defined.

#### **Feedback to the consultation**

193. Almost every respondent supported the proposed definitions as they stand and believed no further definitions should be added to the RTS One respondent suggested for the general approach to the definitions to have a more technology-neutral stance, a fact that has been reflected throughout this report.
194. Another respondent suggested several terms to be included as further defined terms in the definitions of the text to better cover the rapid nature of evolving practices in the crypto assets market. A different respondent suggested clarifying the scope of transactions that would fall under the record keeping requirements.
195. Furthermore, one respondent suggested a clarification of the definition of undertaking a transaction that would reduce the proposed scope which is currently based on the “executing a transaction” definition of RTS22.
196. One respondent asked for the inclusion of general business continuity requirements from the perspective of the CASPs. Another respondent requested to clarify the scope of the recordkeeping requirements as it relates to parties other than the CASP which are involved in the transaction.

#### **ESMA assessment and recommendation**

197. ESMA believes that the approach to the definitions as well as the rest of the fields in the Annex should indeed follow as much as possible a technology-neutral approach and has tried to reflect that throughout this report.

198. As for the suggested inclusion of further definitions to cover the rapidly evolving nature of the market, although the idea is certainly valid, it might be counterproductive to try and overreach when covering terms as these which might be subject to evolution.
199. As regards the definition of undertaking a transaction, the current definition seems more fit for purpose, while the suggested change to the scope could be achieved by clarifying the text in a way that avoids a repetition of the transmission or orders.
200. As for the point concerning the business continuity requirements and their connection to ICT requirements in DORA, although it is a valid point, it does seem out of the scope of these RTS. With regards to the scope of the recordkeeping requirements the respondent merely asked for a clarification on the scope of these RTS applying to CASPs, which does not require the introduction of any new definitions.
201. ESMA therefore suggest keeping the current definitions as they were proposed while accounting for terminology changes related to specific technologies. ESMA sees no need to add any additional definitions to these RTS.

### *Reception and transmission of orders*

#### **Background**

202. Article 3(1), point 23, of MiCA defines the service of reception and transmission of orders as “the reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution”. In order to ensure that the records of transmitted orders are exhaustive enough to empower NCAs to monitor compliance with MiCA requirements along each step of the transmission chain, ESMA is proposing that the transmitting firm should record a list of critical data elements pertinent to the transmitted order.
203. In the case when the CASP transmits the order to a third country entity, where the receiving firm is not governed by MiCA, the transmitting CASP is required to record all details of the order that would otherwise not be recorded.
204. Additionally, ESMA proposes the CASP to record a list of data elements related to the execution of orders on behalf of clients, regardless of whether the transaction is finally conducted outside of EU or not. In particular, the CASP should record the ID of the buyer/seller according to the different use cases. Information on the identity of counterparties involved in cross-border trading activity is particularly relevant to monitor market integrity. This data element would be essential to detect market abuse practices, such as wash trades to inflate the trading volumes of an exchange or a crypto asset.
205. In the Consultation Paper, ESMA first asked the stakeholders whether they anticipate any practical issues with the implementation of the proposed approach to reception and transmission of orders. Following this question, ESMA asked which transaction data would be retrievable in cases where a CASP execute the order on a third country

platform/entity and if the stakeholders anticipate any problems in retrieving the information about the buyer/seller to the transaction.

### **Feedback to the consultation**

206. With regards to the proposed approach to the reception and transmission of orders, the majority of respondents consider that there should not be issues with it, while several respondents noted potential issues when it comes to transmission of orders from 3rd country CASPs or trading platforms. Some respondents signalled that given the fact that 3<sup>rd</sup> country entities would not fall under the scope of MiCA there could be issues both of lack of information provided as well as issues in terms of data standards and formats. Additionally, issues related to technology-related data protection safeties could play a role as part of the reason behind missing information. The transmission and reception of orders from third countries had already been identified in ESMA's Consultation Paper as a major issue when it comes to ensuring the retrieval of the data by CASPs.
207. The approach of allowing CASPs to demonstrate a best effort scenario whenever information from these kinds of orders is missing has been raised by certain respondents as having certain benefits from a supervisory point of view. There is a risk, however that this would lead to lower effort from CASPs to retrieve information from third country parties.
208. Nevertheless, in order to reflect the fact that CASPs will depend on third parties not subject to MiCA to retrieve certain information, ESMA proposes to introduce a requirement to record-keep information stemming from the routing of orders to third country entities whenever this information is retrievable.
209. On another point, certain respondents suggest including a flag signalling the country of origin and destination when applicable while others believe that the buyer seller flag might not be available when dealing with decentralised exchanges. Furthermore, support to the inclusion of all other fields included for EEA undertaken transactions, especially including the use of LEI was expressed by another respondent.
210. Lastly, the majority of respondents agreed that there are likely to be several issues when retrieving information not only concerning the buyer/seller of the transaction, with a special emphasis on transactions involving third countries. Respondents noted that both when it comes to centralized and decentralised exchanges, in many situations, entities or individuals not subject to MiCA would generate a void of information, including but not limited to their lack of obligation to have an LEI.
211. In that line, some respondents noted that mandating CASPs not to allow trading to parties that do not have an LEI would cause severe market disruption.
212. Furthermore, several respondents agreed that due to due diligence and know your customer requirements being different across jurisdictions, CASPs will have issues retrieving some of the information.

213. A few respondents signal the importance of ensuring privacy and the fact that this can both cause lack of information when it comes to transactions involving third countries, but that it should also be ensured as much as possible by avoiding the recording of plain information whenever this can be substituted by anonymised means.

### **ESMA assessment and recommendation**

214. To address the issue of orders transmitted to third countries entities, the final requirements focus on the CASPs' ability to retrieve such information from third parties. This would require CASPs to demonstrate whenever they are objectively unable to retrieve certain/the totality of the information from a third party and that they applied the correct steps to ensure their obligations under these RTS.
215. Since the responses seem to agree on the fact that the same fields are relevant when it comes to transactions executed by CASPs in third countries ESMA suggests maintaining its initial list of proposed fields. A potential additional field covering the country of origin or destination does not seem necessary considering the information can be retrieved via other fields.
216. Furthermore, concerning the LEI requirement, ESMA included a waterfall approach to identification of legal entities in the final requirements. This approach sets the LEI as the default identifier in which a legal entity should be identified and provides for an alternative in case an entity does not have an LEI. Such alternative is allowed provided that it is deemed equivalent and meets certain criteria.
217. Consequently, where the transaction was transmitted to a third country entity for execution on a third country trading platform for crypto assets, the CASP should record the MIC code of the platform or the LEI or alternative equivalent identifier of the platform operator. In the case of a EU CASP directly executing on a third country trading platform, or if the transmitting and receiving firm are part of the same group, the CASP should record the LEI of the counterparty, an alternative legal entity identifier that was deemed equivalent to LEI or, if the counterparty is not eligible for a LEI, the National ID of the counterparty.

### *Methods for client identification*

#### **Background**

218. ESMA suggested to use similar methods for client identification that are used under MiFIR. This would require the CASPs to have appropriate arrangements in place in order to collect and verify the LEI of its client, of those clients that are eligible to obtain one, before the transaction takes place. In particular CASPs must ensure that the length and construct of the code are compliant with the ISO 17442 standard, that the code is included in the Global LEI database and that it pertains to the client concerned. A client who is a legal entity or structure that is eligible for an LEI, including an individual acting in a business capacity, a charity, or a trust, will need to make arrangements to obtain an



LEI code if it wants the CASP to continue to act on its instructions or make a decision to trade on its behalf when MiCA becomes applicable (no-LEI no-trade rule). Concerning clients that are not eligible for a Legal Entity Identifier, ESMA considers that also in this instance the same identification methods as the ones imposed on Investment Firms authorised under MiFID should be applied.

219. In the Consultation Paper, ESMA has asked stakeholders if they anticipate any practical issues in the implementation of these methods for client identification that are used under MiFIR.

### **Feedback to the consultation**

220. More than half of the respondents did not see any practical issues, there is a clear need to implement common methods for client identification. They supported the approach that parties involved in transactions eligible for an LEI should be identified as such. If a party is a natural person, national identifiers should be used as per the approach in other financial legislation (MiFIR), since Firm-specific codes may not provide a unified method for identifying natural persons, potentially hindering uniqueness and market activity regulation.
221. However, some respondents anticipated practical and legal issues linked with the no-LEI no-Trade obligation, such as high administrative burden for customers and CASPs.
222. Two other respondents believe that the approach may hinder DEXs and other decentralized applications, initially designed to preserve the use wallet addresses without personally identifiable data on a public blockchain. These respondents noted that exemptions based on low value transaction thresholds should be considered. However, as mentioned in the PwC study that was commissioned by ESMA<sup>15</sup>, a solution that preserves the use of wallet addresses would be that *“the personally identifiable data obtained during the KYC processes, could be stored off-chain along with a unique identifier for every market participant that has successfully undergone the KYC process at a DLT market infrastructure”*. In this way, the venue could share the encrypted or hashed versions of the data on the Client ID linked to a particular wallet address with the regulator.
223. Another respondent believes that the proposed national identifiers are ineffective due to discrepancies between national set-ups. Using the full name of the customer as identifier is deemed sufficient for record keeping (as it is the case under the current “The travel rule” in the Transfer of Funds Regulation). However, given that the current regulation regarding transfer of fund/travel rule has been reviewed and will be extended to the scope of crypto assets, additional information such as the LEI of the originator, or any other available equivalent official identifier would be required.

---

<sup>15</sup> [ESMA12-2121844265-3183 Report on the DLT Pilot Regime - Study on transaction reporting based on RTS 22 \(europa.eu\)](#)



## ESMA assessment and recommendation

224. ESMA included a waterfall approach to identification of the parties involved in transactions in the final requirements. This approach sets the LEI as the default identifier in which a legal entity should be identified and provides for an alternative in case an entity does not have an LEI. Such alternative is allowed provided that it is deemed equivalent to the LEI and meets certain criteria. Any alternative identifier must fulfil the requirements that were considered necessary for a robust system of identification at international level<sup>16</sup>. Therefore, such alternative will need to be unique, neutral, reliable, open source, scalable, accessible, available at a reasonable cost and subject to an appropriate governance framework. So far, the market supervisors are not aware of any other alternative equivalent identifier that would meet all these criteria. However, the text in the technical standards leaves the door open to a potentially cheaper equivalent for those non-financial entities that may not already have an LEI, should any alternative be deemed as fulfilling the same criteria as the LEI in the future.
225. ESMA will extend the prescribed length of reported addresses (seller, buyer, smart contract, etc.) where using the length of SWIFT standards i.e., 140 characters was suggested.
226. Since no alternative identifiers that can be used in this context have been found so far, ESMA will continue to assess whether there are such alternative identifiers available that can be used in the context of trading in crypto-assets.

### *Short selling flag*

#### **Background**

227. ESMA is aware that certain short selling techniques that are used on traditional trading venues can also be applied to crypto asset trading venues, potentially leading to similar market integrity concerns. These techniques might affect transactions under the scope of MiCA. CASPs are required to flag any such transactions in their records, enabling NCAs to monitor potential excessive exposure. In the Consultation Paper, ESMA has asked stakeholders if they anticipate any practical issues in the implementation of a short selling flag.

#### **Feedback to the consultation**

228. Half of the respondents do not think there are any practical issues. Those who are anticipating practical problems, however, appear to be the result of definitional problems; the responses ask for a clarification of the short selling concept. If a short selling flag results from trading on derivatives, it will not affect services covered by MiCA. But there is some confusion because the ability to lend a cryptocurrency asset makes it possible

---

<sup>16</sup> [FSB Report Global Legal Entity Identifier for Financial Markets - Financial Stability Board](#)

to execute a short sale position. If ESMA refers crypto-asset lending or if different cases, it is requiring additional consideration.

229. Furthermore, flagging for short selling requires constant monitoring, covering all the current techniques might be complex. It can be difficult because of the complexity of short selling for CASPs to appropriately record and report such activities, thus they must modify their systems and procedures.

### **ESMA assessment and recommendation**

230. ESMA clarifies that when it comes to short selling in this context and what kind of transactions would be covered by MiCA it will be consistently applied when the short selling flag comes from trading of derivatives, but not to other asset classes. Given the complexities of crypto asset transactions, it may be difficult for CASPs to modify their systems and procedures to accurately record and report short selling activity. Finally, since disclosing information to the public could disrupt the market, ESMA must determine whether it is for internal record keeping or would be given to the public.

### **5.2.3. Data elements to be included in the records of CASPs operating a trading platform**

#### **Background**

231. Article 76(16) of MiCA mandates ESMA to define a common format for the order records to be maintained by CASPs operating a trading platform. The common format is crucial for NCAs to discharge their market monitoring duties as it ensures that the information to be maintained by CASPs operating exchanges is sufficiently standardised to be compared for the purpose of cross-border surveillance.
232. Additionally, ESMA identified some fields from RTS 22<sup>17</sup> which could be relevant for MiCA, but still may present certain particularities when applied to trading in crypto-assets. Among these are practices such as the routing of orders by a trading platform for crypto-assets.
233. Furthermore, with reference to MiFID II<sup>18</sup>, certain additional fields have been included for record-keeping purposes such as the practice of partially filling orders or fill-or-kill. However, there may exist technical differences that need to be considered on whether they are applicable to orders in crypto assets. ESMA believes that other fields may be affected as well by the different practices performed when trading in crypto assets and wants to ensure that the table of data elements is as complete as possible while

---

<sup>17</sup> Delegated Regulation of 28 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities

<sup>18</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU

acknowledging the relevance of fields between different CASPs as well as to the specificities of trading in crypto-assets.

234. Therefore, in the Consultation Paper, ESMA asked the stakeholders if they consider the data elements that ESMA proposed applicable or irrelevant to trading in crypto-assets, as well as if these data elements for CASP operating a trading platform would be sufficient in order for NCAs to properly perform their supervisory duties. With regards to routed orders, it was asked if the stakeholders believe that a specific definition of routed orders should be provided as it applies to orders that are routed by the trading platform for crypto-assets to other venues. It was also asked if the definition should include CASPs operating a platform which uses only on-chain trading. Regarding the fill-or kill strategies and partially filled order, it was again asked if these are considered applicable for trading on platforms for crypto-assets.

### **Feedback to the consultation**

235. Most respondents agreed with the relevance of the proposed data elements while supporting a uniform approach to data formats. However, a couple of respondents believed that some of the proposed data elements might make the regime too detailed including data fields related to investor protection that might not be relevant for crypto assets markets. Some respondents made reference of their support to the conclusions of the study on DLT Pilot regarding the applicability of certain of the fields to DLT technology.
236. All but one respondent suggested no additional data elements are needed to adequately allow NCAs to exercise their supervisory duties. One respondent reminded the fact that a Refit of the text could allow further fields to be added in case of future need.
237. All but two respondents agreed with ESMA's approach and signalled the importance of having a clear and specific definition of the routing of orders with a preference to orders happening on only on-chain venues being included in this definition. One respondent considered the inclusion of the fields concerning the routing of orders should be enough to allow this information to be available to supervisors.
238. Almost all respondents agreed that fill-or-kill strategies are not only relevant but also very common when trading in crypto assets and therefore expressed their support for their inclusion in these RTS. On their compatibility with partially filled orders, several respondents clarified the fact that these strategies are not compatible and should therefore not be recorded as such when accounting for recordkeeping data. One respondent stated that these strategies might be conflicting with other strategies currently practised by CASPs, without suggesting any changes to reflect that statement.

### **ESMA assessment and recommendation**

239. ESMA suggests following its initial proposed approach to the fields as outlined in the Consultation Paper including the conclusions stemming from the DLT Pilot study and exclude the inclusion of specific instructions for the recording of derivative contracts.
240. ESMA suggest keeping the proposed fields for CASPs operating trading platforms while ensuring proper attention is given to future needs when it comes to supervisory actions by NCAs.
241. ESMA suggests proceeding with the proposed approach of including within the definition of routed orders CASPs operating a trading platform using only on-chain trading as it has been generally identified as relevant for the purposes of the definition of routed orders.
242. Lastly, ESMA suggests maintaining its initial approach of including fill or kill orders as they have been recognized as relevant for trading platforms in crypto assets all while acknowledging their incompatibility with partially filled orders.

#### **5.2.4. Methods for sharing and accessing data between CASPs and competent authorities**

##### **Background**

243. In addition to Article 76(16) of MiCA which mandates ESMA to define a common format for the order records to be maintained by CASPs operating as a trading platform, these CASPs are required to give NCAs direct access to their records according to Article 76(15). Considering the large number of CASPs and possible different models of data access, it may be necessary to standardise the data sharing process to ensure effective and efficient access to data. In particular, if there is no element of standardisation of the records and how it is shared across CASPs and NCAs, it would lead to difficulties for NCAs to adequately perform their market monitoring duties.
244. In the Consultation Paper, ESMA asked the stakeholders what kind of measures (common messages, common APIs, others) they are considering feasible to use in order to share and access data in an efficient manner.
245. Furthermore, to share information with competent authorities, ESMA proposed in the Consultation Paper to use messages based on the ISO 20022 methodology. The ISO 20022 is a financial messaging standard currently being used for data exchange between reporting entities and competent authorities under MiFIR, SFTR, EMIR and other reporting regimes. It is widely spread across the financial sector also in areas outside the remit of ESMA's mandate, for instance for payments. ESMA considered it appropriate to use the same standard for MiCA as well, to reduce the implementation burden for both reporting entities and competent authorities alike. In the Consultation Paper, ESMA asked the stakeholder whether they agree with this proposal of using the ISO 20022 methodology.

##### **Feedback to the consultation**

246. With regards to data access, 13 respondents highlighted the need for harmonized measures to share and access data. Suggestions on concrete measures included APIs (six respondents), S3 buckets (one respondent), and decentralized oracles or blockchain explorer for on-chain data (one respondent).
247. Three respondents supporting harmonization suggested to not set strict rules but general guidelines and allow for some freedom to customize fields and parameters.
248. Furthermore, two respondents specifically mentioned these measures should be defined by ESMA similarly as enabled by the empowerment in Article 26 of MiFIR.
249. Two respondents highlighted that measures in this context should also avoid any misalignment with measures stemming from FIDA.
250. Two respondents argued that the measures should allow for protocols to be recycled and deployed in open source to facilitate the harmonization.
251. One respondent highlighted that measures should allow for backward compatibility, input validation, and encryption. This respondent also highlighted that CASP and NCA staff should be trained to best apply these measures.
252. One respondent, a pan-EU trade association representing a wide range of sell-side market participants mentioned standardized file formats, specifically mentioning the JSON format, would be feasible to ensure effective and efficient access to data.
253. One respondent suggested for these measures to not only take inspiration from the traditional financial sector but also the crypto-asset industry which might offer more suitable solutions which will continue to improve as the industry grows.
254. Four respondents did not suggest any particular model of data access or measures relating to them.
255. Of these, two argued that no measures are required because DLT already makes information transparent, one of which welcomed flexibility on format in RTS but also highlighted RTS appear to be inapplicable to CASPs that only carry out transactions classifiable as crypto-asset transfers between wallets (e.g. fields “buyers” and “sellers” are not suited for this type of transactions). Furthermore, this respondent argued that requirements replicating those of MiFIR would be too burdensome for CASPS and their clientele which are unaccustomed to these types of requirements.
256. One respondent argued to allow for different models to organically develop and notably to avoid burdensome requirements for the production and sharing of data that is not useful to market participants.

257. One respondent did not specifically respond to the question at hand but argued that the record keeping as proposed in the RTS is too burdensome and goes beyond legal basis of MiCA.
258. With regards to the ISO 20022 methodology, most respondents clearly supported the use of messages based on the ISO 20022 methodology for sharing information with competent authorities. One respondent was supportive of the use of ISO 20022 but did not recommend its implementation for these purposes before ESMA allows sufficient time for testing the standard's interoperability with Blockchain systems and their interactions with third-parties (i.e., NCAs in the context of MiCA).
259. One respondent signalled that they had not received confirmation from their members regarding their implementation of this standard when sharing information with competent authorities and would therefore urge ESMA to keep a flexible approach that would not pre-empt the standard that the industry might choose for these purposes.

#### **ESMA assessment and recommendation**

260. Considering the need for harmonization that is recognized by the majority of respondents, the recommendations and cost benefit analysis from the DLT Pilot Regime comparing file-based extraction, API-based extraction, and native access to each DLT<sup>19</sup>, and the results from the MiCA monitoring feasibility study conducted by ESMA<sup>20</sup>, data-requests should be made through a traditional “push” mechanism (i.e., CASPs keeping at the disposal of NCAs relevant data).
261. Considering the broad support by respondents for harmonizing methods to share and access data, ESMA will explore the relevant measures to standardise the methods in which order-book records are made available to NCAs. Given the clear support by respondents, ESMA suggests maintaining its initial proposal of using the ISO 20022 methodology for messages.
262. Furthermore, in the context of the preparatory work on Consolidated Tape Providers (CTP), ESMA commissioned a study on data formats and transmission protocols. The objective of the study, which was published in January 2024<sup>21</sup>, was to identify the best technical solution suitable not only for CTP data collection but also other forthcoming data requesting and reporting regimes. According to the outcomes of the study, JSON emerged as an optimal data format for generic regulatory data-transmission purposes thanks to its simple syntax – which makes it developer-friendly - and its flexibility – which allows to represent complex data structures.

---

<sup>19</sup> [https://www.esma.europa.eu/sites/default/files/2023-10/ESMA12-2121844265-3182\\_Report\\_on\\_the\\_DLT\\_Pilot\\_Regime\\_-\\_Study\\_on\\_the\\_extraction\\_of\\_transaction\\_data.pdf](https://www.esma.europa.eu/sites/default/files/2023-10/ESMA12-2121844265-3182_Report_on_the_DLT_Pilot_Regime_-_Study_on_the_extraction_of_transaction_data.pdf)

<sup>20</sup> ESMA commissioned Gartner in 2023 to conduct a study to examine the design of a centralised monitoring system for Market Abuse Monitoring under MiCA. As part of this study, the best way to access data from CASPs was also examined.

<sup>21</sup> [https://www.esma.europa.eu/sites/default/files/2024-01/ESMA12-437499640-2360\\_Study\\_on\\_data\\_formats\\_and\\_transmission\\_protocols.pdf](https://www.esma.europa.eu/sites/default/files/2024-01/ESMA12-437499640-2360_Study_on_data_formats_and_transmission_protocols.pdf)

263. The study demonstrated that JSON outperforms other formats in several key areas. First, its less verbose syntax ensures higher reliability and ease of use which reduces the likelihood of errors during transmission/reception of information and increases the overall data quality. Additionally, JSON facilitates faster data transmission, through better performances in parsing and serialization speed.
264. While JSON offers numerous advantages, it features also limitations in less critical aspects. Notably, JSON lacks built-in support for certain features, such as inline documentation and digital signatures. However, the absence of inline documentation may not be considered a critical drawback, and although JSON does not provide native support for digital signatures, external libraries can be utilised to achieve this functionality.
265. Finally, ISO 20022, which ESMA suggests as using for messages, is designed to accommodate a variety of data-interchange formats, among which JSON. Therefore, the incorporation of JSON within ISO 20022 underscores its suitability for regulatory reporting, highlighting its alignment with established standards and systems.
266. Consequently, based on the findings of the study, the potential benefits offered by JSON compared to other formats, and the intention to gradually align all regimes requiring transmission of granular structured data on the JSON data format, ESMA considers use of JSON in the context of MiCA as a way to improve the timeliness, accuracy, and overall efficiency of reference data transmission, still ensuring compliance with the ISO 20022 methodology.



## 6 Machine readability of white papers and white papers register

### 6.1 Background and legal basis

**Article 6** (crypto-assets other than asset-referenced tokens or e-money tokens)

[...]

10. The crypto-asset white paper shall be made available in a machine-readable format.

11. ESMA, in cooperation with EBA, shall develop draft implementing technical standards to establish standard forms, formats and templates for the purposes of paragraph 10.

[...]

**Article 19** (asset-referenced tokens)

[...]

9. The crypto-asset white paper shall be made available in a machine-readable format.

10. ESMA, in cooperation with EBA, shall develop draft implementing technical standards to establish standard forms, formats and templates for the purposes of paragraph 9.

[...]

**Article 51** (e-money tokens)

[...]

9. The crypto-asset white paper shall be made available in a machine-readable format.

10. ESMA, in cooperation with EBA, shall develop draft implementing technical standards to establish standard forms, formats and templates for the purposes of paragraph 9.

[...]

267. With regards to the specific format, the mandates included in Articles 6, 19 and 51 require ESMA to define a format enabling machine readability of white papers.

268. The term “machine-readable” is not defined in MiCA itself. However, the Open Data Directive (EU) 2019/1024 and the Regulation on the establishment of a European Single Access Point or ESAP (Regulation (EU) 2023/2859) defines machine readability as

follows: “*machine-readable format*’ means a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure. [...]”. In light of this definition, PDF as well as html are not machine-readable formats, since they do not allow data to be identified and recognised by software applications.

#### **Article 109(8)**

*8. ESMA shall develop draft regulatory technical standards to further specify the data necessary for the classification, by type of crypto-asset, of crypto-asset white papers, including the legal entity identifiers of the issuer and crypto-asset white paper, in the register and specify the practical arrangements to ensure that such data is machine-readable.*

## **6.2 Assessment**

### **6.2.1. Format of the MiCA white papers**

#### *iXBRL format*

#### **Background**

269. In the consultation, ESMA requested feedback on the proposed criteria for identifying a relevant machine-readable format for the MiCA white paper, specifically mandating iXBRL as the standard format, pursuant to the outcomes of an independent study.
270. For those stakeholders who agreed with the iXBRL mandate, ESMA asked whether they also agreed that the white paper should be a stand-alone document with a closed taxonomy, meaning without extensions or complex filing rules. For those stakeholders who objected to the iXBRL mandate, ESMA requested they elaborate on their answers and provide proposals for alternative solutions that would meet the criteria identified in the Consultation Paper (which are based on Level 1 requirements).
271. To understand the current range of practices in non-standardised white papers published by issuers and offerors, ESMA asked if stakeholders have already prepared white papers in a different machine-readable format, and if so, which format. Relatedly, ESMA asked how the MiCA-mandated white paper would differ from any white papers that respondents have drawn up or analysed prior to MiCA. In terms of content, ESMA asked whether any additional information that was previously included in white papers but is no longer allowed under MiCA will continue to be made available to investors, i.e., as marketing communication.
272. Lastly, ESMA asked for opinions on the estimates of the cost of preparing a white paper in iXBRL format. Those who disagreed with the estimate were encouraged to provide their own estimates, excluding the costs of information sourcing, which should be considered as part of the base scenario.

## Feedback to the consultation

273. Most respondents (75%) supported ESMA's proposal to mandate iXBRL for MiCA white papers or agreed to rely on the outcome of an independent study. Some highlighted the use of iXBRL in sustainability reporting, as well as for the preparation of financial statements of issuers' admitted to trading on regulated markets.
274. Some respondents would have preferred allowing preparers to choose the machine-readable format, noting that human readability is not a Level 1 requirement but a "nice-to-have." ESMA emphasised that its mandate requires specifying a format, not leaving it open or to the discretion of market participants (as this would create the risk of non-standardised formats).
275. As it relates to current industry practice, feedback from respondents noted that most white papers are currently in PDF format, as this is most conducive to including graphics and images (needed for the technical nature of the documents in their current form). ESMA pointed out that iXBRL supports graphics and images and noted the legal mandate is for a machine-readable format—not just data extractability.
276. While most respondents did not object to the cost estimate for preparing iXBRL white papers, some raised concerns about the high estimated costs for regulators and the preference for a simpler conversion tool rather than a complex online submission form.
277. Respondents acknowledged the increased standardisation under MiCA, with some highlighting differences in focus, such as more financial and sustainability information compared to previous white papers. ESMA reiterated that these changes are mandated by Level 1 MiCA regulations and that these technical standards are intended to clarify the format, template, and data necessary for classification. The content of the disclosures is out of scope for these draft standards.

## ESMA assessment and recommendation

278. In light of the comments received by stakeholders, ESMA assessed that the draft ITS should not be amended.

### *Proposed template to follow when drawing up MiCA white papers*

## Background

279. In the second consultation package, ESMA requested stakeholder feedback on the proposed template for presenting information in the white papers, including comments on the specific fields, values, and descriptions—particularly where additional explanatory information was provided.
280. Further, ESMA asked whether there were additional data elements in the table of fields that would benefit from further explanatory descriptions with the goal of ensuring that the

information provided by issuers and offerors of crypto-assets is both understandable and comparable across different disclosing entities.

281. ESMA also surveyed stakeholders on whether it would be useful for ESMA to provide an editable template to support preparers of white papers in complying with the proposed format requirements in the draft ITS.

### **Feedback to the consultation**

282. Most respondents agreed that ESMA's proposed template for MiCA white papers is largely effective. There was broad support among respondents for a structured approach to standardising information disclosure in the white papers. Some respondents provided drafting suggestions to enhance clarity and usability. Suggestions included refining field definitions and improving the layout for better legibility.
283. One respondent highlighted practical challenges in filling out information for (Decentralized Autonomous Organizations) DAOs, noting their non-traditional organisational structures. On this point, some respondents sought guidance for the fields such as, "Members of the management body," especially for entities without formal management structures (e.g., foundations or decentralised projects).
284. Other feedback on the specific fields included objections to making telephone numbers mandatory fields for privacy reasons. Some respondents argued against requiring an LEI or national identifiers from smaller issuers. ESMA clarified that it cannot remove fields mandated by MiCA in Level 1, even if certain fields seem unnecessary or burdensome for specific issuers. However, it should be noted that the final draft includes the possibility for issuers / CASPs to provide an alternative equivalent identifier, provided that it fulfils the criteria set out in the Regulation.
285. Other proportionality concerns included the suggestion that MiCA's Level 1 provisions (such as recital 24) were not adequately considered. Here, ESMA reiterated that its role is to specify a machine-readable format as per MiCA Level 1, which limits flexibility in accommodating exceptions for unique types of crypto-assets.
286. Stakeholders also called for more detailed guidelines or examples to ensure uniformity in reporting across a diverse set of crypto-assets. In particular, respondents requested further clarification on liability for disclosed information, particularly when preparers are not the issuers but the offerors. Questions also emerged about the applicability of certain fields to all types of crypto-assets, considering their varying legal structures and operational models.

### **ESMA assessment and recommendation**

287. In light of comments received, ESMA has made some editorial changes to the white paper templates but does not deem it necessary to change its overall proposed approach. The most significant change that was implemented in the template is the

addition of a section named “description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register”. ESMA deemed it relevant to leverage on this field to add the requirement on CASP/issuers to provide certain metadata which are necessary for the set-up of the register ESMA is required to develop by Article 109 of MiCA. This is because many of the data NCAs need to provide to ESMA for the purpose of the register will need to be provided by CASPs/issuers and it was deemed beneficial to harmonise the way this data will be provided to NCAs via the white paper to ensure smooth implementation of the ESMA register and ensure that it is clear to stakeholders what is the full set of data that will need to be reported. This also ensures that CASPs/issuers will not face ad hoc data requests from NCAs but will be able to discharge all their obligations via the white paper only.

288. With regards to the editable template, in light of the support to the proposal, ESMA will provide support to CASPs and issuers by providing an editable template for the preparation of an iXBRL white paper.

## **6.2.2 Data elements necessary for the classification of crypto-assets and white papers pertaining to those crypto-assets**

### **Background**

289. In the Consultation Paper, ESMA specified certain metadata that would be required in order to make white papers easily researchable through its database. This also takes into the consideration the need to ensure consistency with the metadata which will be required under the European Single Access Point (ESAP) framework, where the white papers will need to be made available in the future, so as to ensure that no additional metadata will be required in 2030 when the white papers will need to be made available to ESAP directly.
290. To ensure the identification and the classification of the white papers in ESMA register, ESMA has proposed that, where available, a valid ISO 24165 Fungible Functional Group Digital Token identifier (FFG DTI) and the more granular DTIs pertaining to the crypto-asset(s) referred in the white paper should be provided as part of the metadata. Such granular DTI identifiers will enable regulators to unambiguously link the crypto-asset white paper with the relevant blockchain where the instrument is issued/traded/settled.

### **Feedback to the consultation**

291. Respondents suggested additional attributes deemed as relevant for the comparability of white papers, including: provisions fostering comparability for investors; the governance structure and mechanisms; last update date and version number; auditing firm’s name; tokenomics; the exchange ticker. in addition to the MIC; roadmap; unique value proposition; detailed consensus mechanism description; risk management practices; compliance status; and developer and management team backgrounds.

292. The proposed requirement to mandate an LEI for eligible entities received very broad support from respondents to the consultation. A specific case of non-eligibility was mentioned: issuers are not identifiable in the case of “decentralized autonomous organisations”. Indeed, there the concept of “issuer” may not apply to this specific case and therefore alternative means of identification for this specific case may be appropriate.
293. Wide support was received on ESMA’s proposal regarding metadata elements. With regards to the metadata on the “industry sector of the economic activities”, it was suggested that the categorisation should be adapted to the digital assets sector and be more granular - e.g. yield farming, gaming, stablecoins, peer-to-peer, payments. However, since this metadata was originally introduced only for the purpose of ESAP and the final text on ESAP does not require crypt-asset issuers and CASPs to report an industry sector, this metadata, as well as the metadata regarding size, have finally been removed from the draft RTS.
294. The sustainability indicators suggested by respondents to allow for comparability and classification between white papers should already be part of the white paper as per the *RTS on content, methodologies, and presentation of sustainability indicators on adverse impacts on the climate and the environment* which is covered in Section 2 of this Final Report.
295. The MIC will be mandated under the *RTS on record-keeping by crypto-asset service providers*, among others, which should resolve the issue raised by a respondent that the exchange ticker would be more likely to be assigned than the MIC.
296. The time and date of the latest update of the white paper is a data element suggested by a respondent which is already present in the draft *RTS on the data necessary for the classification of white papers* (field 21 of Table 2).
297. Finally, the remaining data elements suggested by respondents were not included in the RTS either because they do not fall under the empowerment of ESMA under Article 109(8) or because they were deemed unnecessary for the purpose of the register.

### **ESMA assessment and recommendations**

298. In light of the comments received regarding the metadata elements, and of the ongoing work on the Joint Committee ITSs on Article 5 and Article 7 of the European Single Access Point (ESAP), ESMA has proposed a number of changes to its original draft ITS in order to:
299. Align the requirements in this RTS with those in the JC ITSs on ESAP currently under development
300. Ensure that all data necessary for the registers mandated by Article 109 and 110 of MiCA are made available to ESMA by NCAs.

## 7 Technical means for appropriate public disclosure of inside information

### 7.1 Background and legal basis

#### Article 88 (4) of MiCA:

*“In order to ensure uniform conditions of application of this Article, ESMA shall develop draft implementing technical standards to determine the technical means for*

*(a) appropriate public disclosure of inside information as referred to in paragraph 1; and*

*(b) delaying the public disclosure of inside information as referred to in paragraphs 2 and 3.”*

301. Title VI of MiCA establishes rules to deter market abuse with respect to trading of crypto assets. As part of these rules, MiCA prohibits insider dealing, unlawful disclosure of inside information, and market manipulation and includes an obligation to publicly disclose inside information.
302. One of the pillars of MiCA’s market integrity provisions is the definition of inside information, which is defined in Article 87 of MiCA as: *“information of a precise nature which has not been made public, relating, directly or indirectly, to one or more issuers, offerors or persons seeking admission to trading, or to one or more crypto-assets, and which, if made public, would have a significant effect on the prices of the relevant or related crypto assets”*.
303. Article 88(1) of MiCA requires issuers, offerors or persons seeking admission to trading to inform the public as soon as possible of inside information that directly concerns them, in a manner that enables fast access as well as complete, correct and timely assessment of the information by the public. The same provision requires the relevant parties to post and maintain on their website, for a period of at least five years, all inside information that they are required to publicly disclose.
304. Article 88(2) of MiCA establishes that issuers, offerors or persons seeking admission to trading can delay the disclosure of inside information where immediate disclosure would be likely to prejudice a legitimate interest of the relevant party, and if the delay of the disclosure is not likely to mislead the public and the confidentiality of the information is ensured.
305. In cases where NCAs suspect issuers, offerors or persons seeking admission to trading of not properly disclosing inside information, NCAs may seek remediation through the supervisory and investigative powers listed in Article 94. In addition to these general supervisory powers for NCAs, MiCA in Article 111 (5) also lists specific sanctions for breaches of Article 88. These sanctions include maximum administrative fines of EUR 1m for natural persons and EUR 2.5m for legal persons.



306. With respect to the disclosure of inside information, Article 88(4) of MiCA mandates ESMA to develop a draft ITS to determine the technical means for (i) appropriate public disclosure of inside information and (ii) delaying the public disclosure of inside information.
307. In the Consultation Paper referring to this mandate, ESMA consulted on the draft ITS on technical means for appropriate public disclosure of inside information (Section 8).
308. ESMA has developed the draft ITS considering the similarities between the MAR and MiCA legal texts regarding inside information, its disclosure and the cases for delayed disclosure. Furthermore, ESMA saw merit in aligning the regime for disclosure of inside information under MAR and MiCA to leverage on the experience developed under MAR and streamline the regulatory framework on inside information disclosure. Hence, the MiCA draft ITS has been largely based on the MAR ITS, with the addition and adaptation of some provisions targeting features which are specific to the crypto environment.
309. The consultation phase ran from 5 October to 14 December 2023. Taking into account the feedback received during the consultation phase including reactions to the Consultation Paper, direct one-on-one interactions with stakeholders, as well as advice from the SMSG, ESMA now presents its final draft ITS.

## 7.2 Assessment

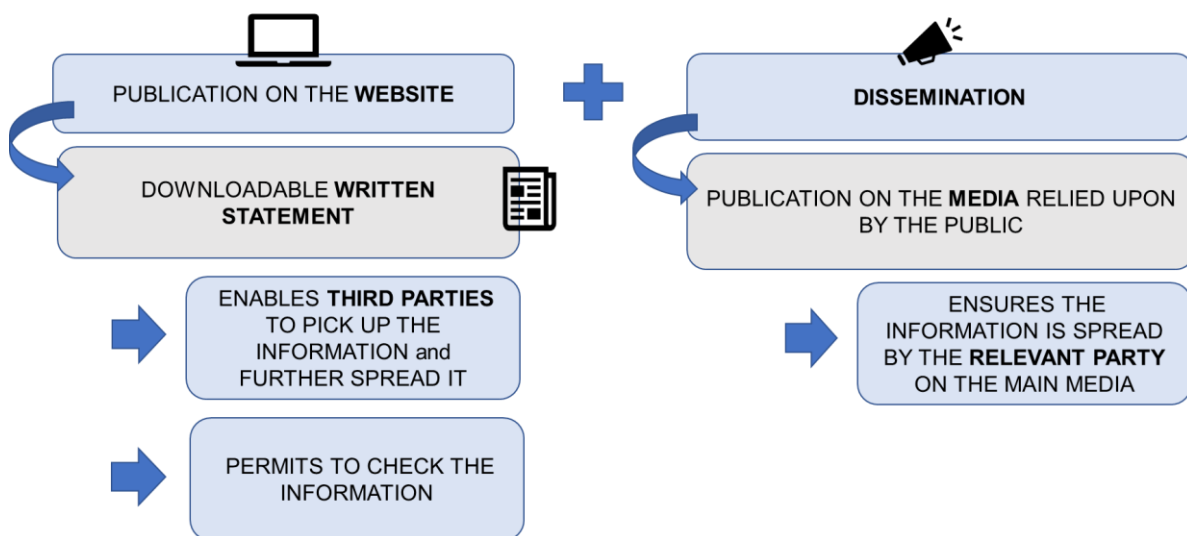
### 7.2.1 General provisions and terminology

#### Background

310. In Section 8 of the Second CP on MiCA, ESMA analysed the obligations to disclose inside information enshrined in Article 88 of MiCA.
311. In this respect, ESMA noted that the first part of Article 88(1) of MiCA requires issuers, offerors, or person seeking admission to trading to “*inform the public as soon as possible of inside information*” (i.e. **active dissemination**), while the last sentence of the same paragraph provides for inside information to be posted and maintained on the website of the relevant party (i.e. **publication on the website**).
312. ESMA considered that publishing information simply by making it available on the website and leaving to the public the duty to retrieve it would not be sufficient to ensure fast access by investors. Therefore, ESMA concluded that active dissemination of inside information and its publication on the website are two separate obligations, meant to achieve different objectives.
313. In particular, ESMA noted that while active dissemination ensures a wider distribution of the information through the media that are used by the public to retrieve information, on the other hand, the publication on the website represents a reliable source against which all the other media publications can be checked.

314. On this basis, the draft ITS proposed in the CP addresses separately the posting of inside information on the website of the issuer, the offeror or the person seeking admission to trading (Article 2 of the draft ITS) and the technical means on disclosure of inside information (Article 3 of the draft ITS).
315. To enhance clarity of the obligations contained in the draft ITS, Article 1 of the draft ITS defines few terms, notably “alert”, “durable medium”, “electronic means”, “social media”, “web-based platforms” and “trading platforms for crypto assets”.

**FIGURE 1: OBLIGATIONS FOR RELEVANT PARTIES TO DISCLOSE INSIDE INFORMATION**



### Feedback to the consultation

316. Respondents to the consultation were supportive of the approach adopted and of the listed definitions. However, a few respondents asked for clarifications of terms or provisions contained in MiCA or in the draft ITS.
317. With respect to MiCA, questions focused on the definition of “**inside information**” contained in Article 87. To better understand when the disclosure obligation arises, respondents asked (i) when inside information has a “**significant effect on the prices**” and (ii) how to interpret the requirement for inside information to “directly concern” issuers, offerors or persons seeking admission to trading, where the information is available to more than one of these persons.
318. Few respondents commented that the term “inside information” appears to be vague and that further clarifications specific for the MiCA context would be welcome, especially in the form of examples or explanatory notes.

319. One respondent commented the definition of “**offeror**” contained in Article 3(13) of MiCA. He noted that the term refers to a person who “offers crypto asset to the public”, and that it could thus be interpreted to include operators of the trading platforms. He asked to clarify who is subject to the disclosure obligation.
320. With respect to the terms contained in the draft ITS, one respondent asked to specify what the “**media which are reasonably relied upon by the public**” are indicating this is quite a vague wording. Another respondent asked to better define “**durable medium**” to ensure that the way information is stored and retained meets the standards outlined in the regulations. Clarifications were also asked on how the term “**social media**” and the “**web-based platforms**” should be interpreted in the MiCA context.

### **ESMA assessment and recommendation**

321. In view of the general support by stakeholders for the definitions listed in the draft ITS, ESMA maintained Article 1 of the draft ITS unchanged.
322. With respect to the clarification request on the definitions of “inside information” and “offeror” ESMA notes that such terms are defined directly in L1 (MiCA). As a result, ESMA cannot amend the relevant definitions through an ITS.
323. For the sake of clarity, however, ESMA recalls that Article 87(4) of MiCA indicates that by information which would likely have a significant effect on the prices of crypto-assets it is meant information that “a reasonable holder of crypto-assets would likely use as part of the basis of the holder’s investment *decisions*”.
324. In addition, ESMA notes that the persons mentioned in Article 88 of MiCA (i.e. issuers, offerors and persons seeking admission) are all subject to the disclosure obligation. As a result, whenever any of those persons is in possession of the inside information, they are required to proceed with the disclosure as soon as possible.
325. It should be noted that after public disclosure the information is no longer inside information, and the other persons who are in possession of such information are not subject to the disclosure obligation.
326. With respect to the definition of “offeror” (Article 3(13) of MiCA), ESMA recalls that it should be read in conjunction with the definition of “offer to the public”. In particular, Article 3(12) of MiCA identifies the offer to the public as a separate and different activity from the “operation of a trading platform for crypto assets” (defined in turn in Article 3(18) of MiCA). As a result, it is unlikely that the offeror and the trading platform could be confused in respect to the disclosure obligation.
327. As to the term “**media which are reasonably relied upon by the public**”, ESMA would like to recall that Article 3(2) of the draft ITS indicates that such media include, social media, web-based platforms and trading platform for crypto assets. ESMA also recalls

that the terms social media, web-based platforms and trading platform for crypto assets are all defined in Article 1 of the draft ITS.

328. For completeness, ESMA clarifies that media reasonably relied upon by the public may also include traditional media (e.g. newspapers). To enhance clarity on this point, Article 3 of the draft ITS has been amended to include traditional media in the list of possible media which are reasonably relied upon by the public (see below Section 7.2.3 on means for public disclosure of inside information/active dissemination).
329. In addition, a recital has been added to the draft ITS to clarify that to ensure that the inside information is disseminated to an as wide public as possible, entities subject to the disclosure obligation should consider making use of more than one type of media whenever a single one is not deemed to be sufficient. The same recital also clarifies that the requirement to use the “media reasonably relied upon by the public” involves that the use of only one type of media with a limited reach cannot be considered valid to comply with the obligation (e.g. social media with a limited number of users).
330. With respect to “**durable medium**”, ESMA considers the current definition (referring only to requirements for the medium) as sufficient to align the activity of the NCAs for the purpose of record keeping. On the contrary, ESMA consider that it would be disproportionate to identify the specific electronic means to be used for this purpose.
331. Lastly, ESMA would also like to recall that questions for clarifications on the practical application or implementation of MiCA can be submitted to ESMA through the ESMA Q&A tool<sup>22</sup>, pursuant to Article 16(b) of ESMA Regulation. ESMA thus invites market participants to submit questions on application of terms used in MiCA through this channel.

## 7.2.2 Posting of inside information on the website of the issuer, the offeror or the person seeking admission to trading

### Background

332. With respect to the publication of information on the issuer’s website, in the Second CP on MiCA, ESMA proposed that the inside information should be published in the form of a downloadable written statement, with the purpose of allowing third parties (e.g. journalists) to further spread the information.
333. Overall, the requirements proposed in Article 2 of the draft ITS are equivalent to the ones already contained in the MAR ITS. Those aim, among others, to ensure free of charge access to information and ease the identification of the relevant information on

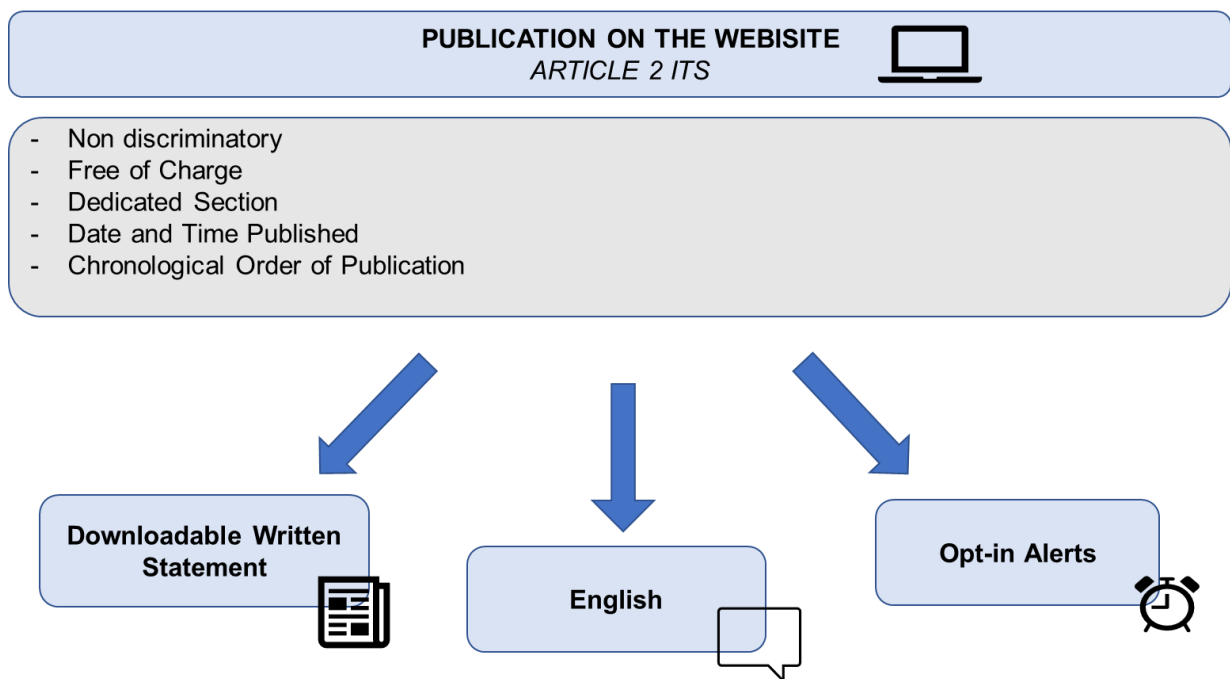
---

<sup>22</sup> [Questions and Answers \(europa.eu\)](https://europa.eu)

the website. That Article additionally includes some requirements aimed at facilitating access to the information by the public.

334. Considering the cross-border dimension of trading of crypto assets, Article 2 of the draft ITS proposed that the relevant information should be published on the website either in the language in which the white-paper of the crypto-asset is drawn up or, where feasible, in a language customary in the sphere of international finance, i.e. currently English.
335. To further facilitate transmission of inside information, it was also proposed that the website of the issuer, the offeror or the person seeking admission to trading should enable push notifications or alerts for investors on any new publication of inside information, with the purpose of enabling fast access to information.

**FIGURE 2: PUBLICATION ON THE WEBSITE**



### Feedback to the consultation

336. In the Second CP on MiCA, ESMA asked stakeholders if they agreed with the proposed requirements for publication of the inside information on the website of the issuer, offer or person seeking admission to trading, and if they would support any additional requirement regarding the publication on the website.
337. The large majority of respondents supported the proposed requirements. Few respondents highlighted that additional specifications would be desirable, as for example a uniform template for the publication of information or features enhancing the accessibility of the published information (e.g. archiving and historical search functions).

338. A minority of respondents highlighted that not all issuers, offerors or person seeking admission to trading might have a website, hence it could be desirable to envisage alternative possibilities for publishing inside information, for example through platforms comparable to a regulatory news service (RNS).
339. ESMA additionally asked stakeholders their views regarding the requirement to allow push notifications regarding the publication of inside information from the website of the issuer, offeror or person seeking admission to trading to the public subscribing to such alerts.
340. The large majority of respondents did not see any obstacle for the website of the relevant parties to allow for specific alerts. A minority of respondents were not in favour of such requirement for various reasons, including the fact that such alerts might provide an advantage to low latency users and users who base their trading decisions on automated signals, possibly triggering volatility in the market.

#### **ESMA assessment and proposal**

341. With respect to the requirement envisaged in Article 2 of the draft ITS regarding publication of the inside information on the website of the relevant parties, ESMA notes that the majority of respondents supported such proposal.
342. In this respect it should be noted that Article 88 of MiCA states that issuers, offerors and persons seeking admission to trading should post on their website all inside information that they are required to disclose publicly. Hence, ESMA notes that the L1 requires all issuers, offerors and persons seeking admission to trading to have a website for the purpose of publication of inside information. As a result, the case where the issuer, offeror or persons seeking admission to trading do not have a website shall not occur.
343. With respect to the feedback received on the use of alternative means for publishing inside information (e.g. platforms comparable to regulatory news services), ESMA notes that Article 3 of the draft ITS already provides for the use of the website of the trading platform for crypto assets where the crypto-asset is traded as a possible additional means of disclosure.
344. As to the feedback received on further defining a uniform template for the publication of inside information, ESMA notes that prescriptive requirements in this sense would go beyond the legal mandate in Article 88(4)(a) of MiCA. According to Article 88(4), ESMA is mandated to develop an ITS to specify the technical means for the appropriate public disclosure of inside information and providing a uniform template for the purpose of such disclosures would exceed the mandate.
345. ESMA notes that the majority of respondents supported the requirement prescribing that the website of the relevant parties should provide users with the possibility to receive alerts whenever inside information is published.

346. ESMA also acknowledges the views that a minority of stakeholders expressed on automated notifications providing a possible advantage to low latency traders. Nevertheless, it should be considered that once the information is published on the website, the general public would be able to access to it, and any party could envisage automated means to source the information. Hence, on balance ESMA proposes to keep the current drafting of Article 2 of the draft ITS unchanged.

### 7.2.3 Means for public disclosure of inside information (active dissemination)

#### Background

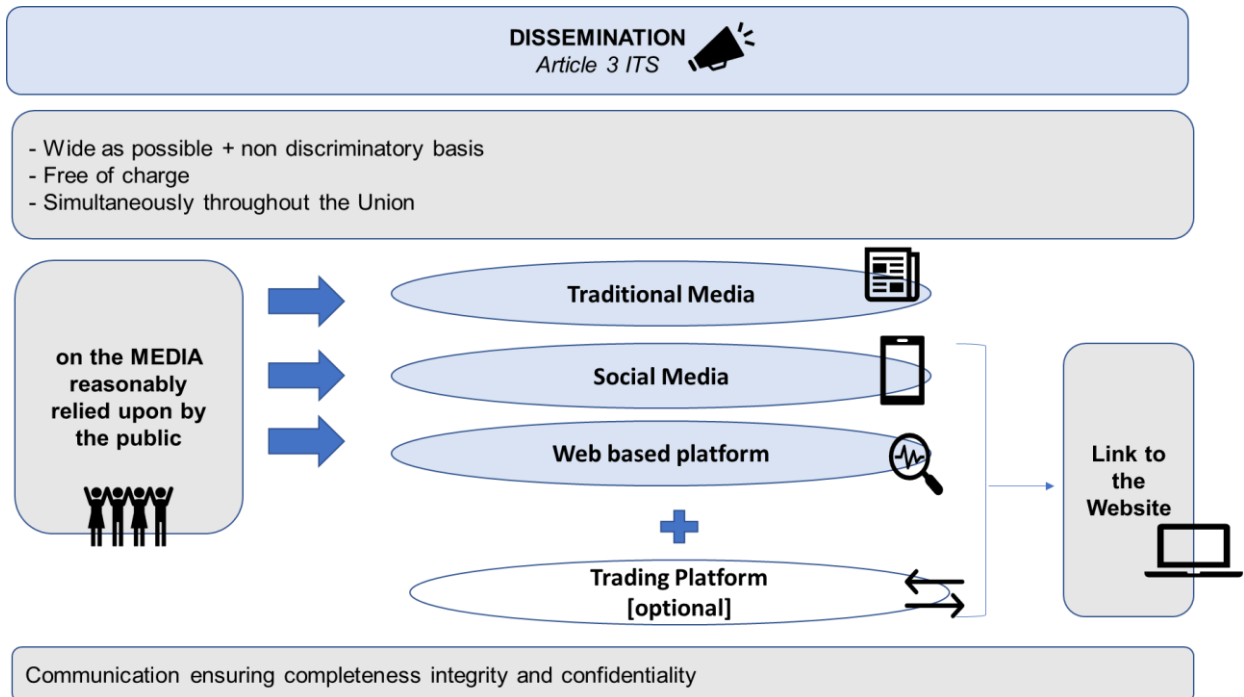
347. Article 3 of the draft ITS describes the general requirements for the dissemination element of the mandate, which requires issuers, offerors and persons seeking admission to trading to disclose inside information by means that ensure dissemination to the widest public possible, on a non-discriminatory basis, free of charge and simultaneously throughout the EU. As part of this obligation, the information must be communicated to the media which are ‘reasonably relied upon by the public.’ See Figure 3 below for a visual overview of the technical means for public disclosures and dissemination.

348. In the draft ITS, ESMA proposed departing from the MAR ITS by incorporating social media and the so-called ‘web-based platforms’ as categories of media ‘reasonably relied upon by the public’ among investors in the crypto-asset market. These new categories can only meet the ‘reasonably relied upon’ standard if they are open and freely accessible (e.g. not requiring invitation). To allow consumers of this information to ensure the authenticity of the information posted, the ITS requires that publication on social media and web-based platforms include a link to the website of the disclosing entity where the original disclosure is published.

349. Additionally, the draft ITS envisages that if the trading platforms where the crypto-asset is listed allow third parties to post information on their websites for dissemination purposes, then this can be an optional (additional) method for dissemination of inside information. The latter is envisaged as a possibility and not as a duty and it is aimed at promoting the publication of inside information in a more centralised manner, under the assumption that investors may more easily come across information that is posted on the same platform where they intend to trade. As for the media, dissemination on a trading platform’s website should also include a link to the website of the disclosing entity where the written statement is published.

350. In the CP, ESMA surveyed market participants about the media they consider investors most likely to rely upon when seeking information about crypto-assets as well as the tools they already use to communicate with investors or clients. ESMA also asked market participants to identify any risks they see when using social media or web-based platforms to disseminate information about crypto-assets and whether they still consider dissemination through traditional media an important channel to include in the ITS.





## Feedback to the consultation

351. Respondents provided examples of the types of media that are prevalent in the information ecosystem of the EU crypto-asset market as well as specific (named) sources for crypto news across these types of media. Throughout these responses, there were indications of confusion about which media would be mandatory vs. optional channels for dissemination and what it would mean for compliance with the ITS.
352. As it relates to compliance, several respondents argued that demonstrating that an issuer or offeror has met the dissemination requirements in Art. 3(5) of the draft ITS (assurance of completeness, integrity, and confidentiality of the information maintained during transmission) would be difficult.
353. Some respondents confirmed the requirement in the draft ITS that regardless of the type of media employed to meet the dissemination obligation, those media should be non-discriminatory and free to access. Many respondents also emphasised the importance of allowing for flexibility in how an issuer or offeror may interpret the 'media reasonably relied upon by the public' for the purpose of broadcasting their disclosures.

### *Traditional media*

354. Examples of traditional media consumed by crypto market participants included crypto-specific trade journals as well as major international news outlets who have in recent years expanded their financial markets coverage to include crypto assets.

355. Traditional media (e.g. stock market newswires) were supported by respondents as means of dissemination (despite low interest from crypto investors) because of the credibility of such platforms, which tend to have stronger editorial standards around what can be published. One respondent also argued that mandating dissemination through at least traditional media would be ideal and perhaps preferable to the multichannel approach described in the ITS, because this would limit unfair information advantages for those investors who are ‘in the know’ about which social media channels to follow for the latest breaking news. By contrast, one respondent said that traditional media are obsolete for reaching crypto investors and therefore would not meet the standard of ‘media reasonably relied upon by the public’.
356. Several respondents noted the more reliable journalistic standards and fact-checking processes built into the traditional media model, which has the consequence of making dissemination through such channels slower compared to other types of media. Another respondent cited the limited reach of traditional media compared to certain types of digitally-native media as a strong rationale for the inclusion of new types of media in the draft ITS (subject to reliability standards).
357. Although none of the respondents in this section raised concerns about the omission in Article 3 of the ITS of any specific reference to traditional media as a means for public disclosure, there was a comment related to this in the definitions section of the consultation feedback (see paragraph 320). ESMA considers a clarification on traditional media a practical addition to that article (see the proposal in the next section).

### *Social media*

358. The four most commonly cited social media platforms for aggregated news on crypto market developments included X (formerly Twitter), Reddit, Telegram and Discord. Respondents also mentioned classic forums, such as ‘Bitcointalk’, as a source for crypto investors. The consensus view of the comments was that crypto investors have come to expect information to be shared on social media platforms, including updates, announcements, and important developments regarding specific services or crypto-assets.
359. Respondents shared mixed views about the inclusion of social media and other web-based platforms as dissemination channels for inside information. Even those who did support its inclusion warned about the difficulty of verifying whether the information published via these channels comes from official sources and the potential for abuse, which could exacerbate market volatility. However, the majority of respondents reasoned that the inclusion of social media as an optional element in an omnichannel approach would enable them to meet the standard of ‘media reasonably relied upon by the public’, especially when considering that only a few crypto investors consume traditional media.
360. As discussed, a major concern raised by several respondents was the veracity and/or authenticity of information available on social media. These respondents cited the threat

of misinformation from fake or unverified accounts as an obstacle to effective disclosures over social media. Despite these concerns, there was still broad support for the inclusion of social media, with caveats about how they should be used to meet the standards for disclosure listed in the draft ITS. To counter misinformation, respondents recommended that investors only consume information from verified sources that link back to the website of the issuer (a requirement already included in the draft ITS for all dissemination channels). Here, respondents also noted that the IOSCO standards on digitalisation of retail marketing and distribution<sup>23</sup> may serve as a guide for how CASPs should approach social media, especially with regards to validation of information posted on such platforms.

361. Only one respondent objected to the inclusion of social media, arguing that it may have the unintended effect of excluding some investors from accessing information or lead to the mixing of disclosures with other unrelated marketing materials. That respondent called for alignment between the means for public disclosure used under MiCA and MAR considering many market participants may be subject to both regulations.
362. To facilitate compliance with the requirements in Article 3 of the draft ITS, one respondent suggested that ESMA develops a set of standards that issuers and offerors could use to allow them to confirm whether the platform or media they intend to use for dissemination has sufficiently developed moderation and curation systems in place to ensure the accuracy and reliability of the information shared.

#### *Web-based platforms & websites of the CASP trading platform*

363. In the category of web-based platforms, respondents identified crypto market data aggregators and/or price-tracking websites (e.g. CoinMarketCap, CoinGecko) as some of the most commonly used platforms for disseminating information to investors. One (crypto-native) respondent noted that they do not see widespread use by retail investors of professional or subscription-based platforms (for financial advice or real-time data).
364. Two respondents endorsed ESMA's approach, confirming that the websites of CASP trading platforms should be considered 'reliable' sources of information, considering they would be regulated entities. Where there was a possibility of so-called 'opt-in' or 'push' alerts about a given crypto-asset or service provider, one respondent said these were often available through an 'in-app' messaging system whereby issuers can tailor their updates directly for followers of their crypto-asset. These alerts can be tailored by investors from a CASP website, however one respondent called on ESMA to exercise caution with this approach and to not impose unnecessary burdens on CASP trading platforms to provide such an alert system which may ultimately subject investors to spam.

---

<sup>23</sup> IOSCO, [Report on Retail Distribution and Digitalisation](#) (FR/12/2022), October 2022

365. Respondents to the consultations indicated that they do not consider it necessary to add any means of communication for the purpose of disclosure to those already prescribed in the proposed draft ITS. However, one respondent suggested to use newsletters or direct notifications via app for the purpose of dissemination in order to ensure fast, direct and prompt communication with investors. Another respondent invited to consider the creation of a communication platform to collect and share inside information with investors.

### **ESMA assessment and recommendations**

366. ESMA notes that the consultation feedback to the questions related to Article 3 of the draft ITS largely endorsed the approach taken by ESMA. In particular, respondents supported the explicit inclusion of social media and web-based platforms as options for dissemination that would meet the ‘media reasonably relied upon by the public’ standard. They also welcomed the additional option of websites of the CASP trading platform, where available.
367. As for the concerns raised by respondents about ability to comply with the dissemination requirement in Article 3(5) of the draft ITS, ESMA understands that reliance on third parties for dissemination may raise risks for the confidentiality of information in transmission. Here ESMA would expect issuers and offerors to ensure the confidentiality of their disclosures using standard measures to mitigate such risks from interacting with third parties (e.g. encrypted email).
368. In view of the broad support among respondents for the proposed means for public disclosure in Article 3, ESMA does not recommend any substantive rewrites to the draft ITS. However, ESMA has made one addition to Article 3(2) based on input from a respondent who questioned the omission of ‘traditional media’ from the provision when it discussed media for ‘effective dissemination’. This update to the text, which now explicitly includes traditional media as an acceptable means for effective dissemination (whereas before it was only implied), should provide more clarity for market participants.
369. As it relates to authenticity or accuracy of information disseminated via social media, ESMA considers the concern already addressed. Given the requirement that issuers or offerors link to the original written statement published on their website when disseminating a disclosure on social media or web-based platforms, there should be no confusion about the provenance of such disclosures. In other words, this requirement should address any verification issues by allowing investors to confirm in real-time the original source of the information. The mandate in this ITS is simply not capable of addressing the many limitations of information-sharing in a social media context that are not unique to disclosures of inside information.
370. In addition, the suggestion from one respondent to have ESMA develop guidance for a minimum set of content moderation standards that a social platform or media outlet should adhere to would not solve the underlying issue. Creating standards for content moderation is not part of ESMA’s mandate and it would apply additional burden on

issuers or offerors when they should be left to their own judgement about how best to reach the interested public.

371. While ESMA appreciates the reference to the 2022 IOSCO measures for the use of social media in digital offerings, the scope of the ESMA mandate in the ITS is not relevant to marketing. In the draft ITS, social media is included only as a tool for dissemination of disclosures. It is also not envisioned that video-based social media (e.g. Tik Tok and YouTube) would be appropriate for the requirements in the draft ITS considering the information should be posted on social media “permitting publication in written form”.
372. With respect to the suggestion to use apps or newsletter to communicate directly with investors, ESMA recalls that point (e) of Article 2(2) of the ITS already foresees the possibility of receiving alerts when the information is published on the website of the issuer.
373. On the creation of a platform to collect and share inside information, ESMA notes this objective is already pursued through the European Single Access Point project (‘ESAP’) <sup>24</sup>. In particular, Article 18 of the Regulation amending certain regulations as regards the establishment of the ESAP <sup>25</sup> foresees the publication of inside information to be disclosed under Article 88 of MiCA on the ESAP starting from 10 January 2030.

## 7.2.4 Delayed disclosure of inside information

### Background

374. In the CP, ESMA analysed Article 88 of MiCA which requires an issuer, offeror or a person seeking admission to trading who has delayed the disclosure of inside information to (i) inform the competent authority of the existence of the delay and (ii) provide a written explanation of how the conditions allowing delayed disclosure were met.
375. In this respect, Article 4 of the draft ITS proposes to prescribe to issuers, offerors or persons seeking admission to trading (i) how to store selected information pertaining to the delayed disclosure and (ii) how to notify the relevant NCA.
376. To promote the standardization of the information, Article 4 of the draft ITS includes a list of elements, analogous to the ones envisaged under MAR ITS, which should be included in the notification.

### Feedback to the consultation

---

<sup>24</sup> The ESAP project entails the creation of a single internet portal run by ESMA to improve access to all information made public by regulated entities. For further information see Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability available here: <https://eur-lex.europa.eu/eli/reg/2023/2859/oj>

<sup>25</sup> Regulation (EU) 2023/2869 of the European Parliament and of the Council of 13 December 2023 amending certain Regulations as regards the establishment and functioning of the European single access point available here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R2869>

377. Respondents in the consultation agreed with the technical means as proposed.
378. One respondent suggested to clarify that if a Member State requires that the explanation of how the conditions for delay are met is to be presented only upon request of the NCAs, issuers, offerors and persons seeking admission to trading are not expected to present such record unless requested.

### **ESMA assessment and recommendations**

379. In view of the general support by stakeholders in respect to the means for delayed disclosure of inside information, ESMA maintained Article 4 of the draft ITS unchanged.
380. ESMA considers that Article 88(3) of MiCA is already clear on the fact that when the Member States have provided that the record of the explanation regarding the delay shall be provided only upon request, in lack of the NCAs request, the record does not need to be provided. As any further indication in this respect would appear as a mere repetition of L1, ESMA did not consider necessary any further clarifications in the ITS on the point.

## 8 Annexes

### 8.1 Annex I: Cost-benefit analyses

#### 8.1.1 RTS on content, methodologies, and presentation of information in respect of the sustainability indicators in relation to climate and other environment-related adverse impacts

*Impact of the draft RTS under Article 6(12), Article 19(11), Article 51(15), and Article 66(6) of MiCA*

1. As per Article 10(1) of Regulation (EU) No 1095/2010, any draft regulatory technical standards developed by ESMA are to be accompanied by an analysis of ‘the potential related costs and benefits’ of the technical standards, unless such analyses “are highly disproportionate in relation to the scope and impact of the draft regulatory technical standards concerned or in relation to the particular urgency of the matter”.
2. The following section outlines ESMA’s assessment of the main policy options included in these draft RTS further specifying the requirements for sustainability indicators to be disclosed by persons drawing up a crypto-asset white paper and CASPs.

##### *Problem identification*

3. As citizens and policymakers alike become increasingly aware of the environmental (as well as social, and governance-related) impacts of financial decisions, the sustainability impact of investments is becoming a more and more important element of investor awareness throughout the financial sector. As this becomes a part of investors’ decision-making, so too rises the risk of greenwashing. With this in mind, the European Union is progressively developing the framework as regards the sustainability-linked aspects of investments within its jurisdiction.
4. In the area of crypto-asset markets in particular, the relatively energy and materials-intensive nature of the technology used implies that (i) there may be a significant sustainability impact of the consensus mechanisms used to issue tokens and validate and record transactions in relation to them and (ii) this impact may differ significantly from one consensus mechanism to another.
5. The lack of standardised information on the adverse environmental impact of crypto-assets would hinder the level playing field and lead to increased risk of greenwashing or retention of information that may be relevant for investors. Against this background, MiCA mandates the disclosure of information on sustainability impacts in the white papers and on the website of CASPs, while ESMA is tasked with further specifying the detailed content, methodology, and presentation of the information in respect of the



sustainability indicators in relation to climate and other environment-related adverse impacts.

#### *Policy objectives*

6. The objective of these draft RTS is to foster investor awareness by further specifying the information that persons drawing up a white paper and CASPs need to disclose in relation to the adverse environmental impact of the consensus mechanisms used as regards the crypto-assets they are offering and in regards to which they are providing services, respectively.

#### *Baseline scenario*

7. In a baseline scenario without the draft RTS:
  - i. persons drawing up white papers would be required to include in the white paper “information on the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue the” crypto-asset, asset referenced token, and e-money token” (Articles 6(1)(j), 19(1)(h) and 51(1)(g) of MiCA respectively);
  - ii. CASPs would be required to “make publicly available, in a prominent place on their website, information related to the principal adverse impacts on the climate and other environment-related adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue each crypto-asset in relation to which they provide services, information that may be obtained from the aforementioned crypto-asset white papers” (Article 66(5) of MiCA), and more generally they would be required to “provide their clients with information that is fair, clear and not misleading [...] (Article 66(2) of MiCA)
8. Persons drawing up a white paper and CASPs would in such a scenario be subject to disclosure requirements with limited harmonisation. Thus, each actor would choose what information to disclose, what methodology to use to calculate any relevant indicators, and how to present this information, which would render it very difficult to ensure comparability across entities’ disclosures.
9. In addition, many tokens are issued using the same consensus mechanisms. Where multiple entities are disclosing information relating to the same consensus mechanism, they could in this scenario disclose different information about the same consensus mechanism, resulting in further confusion for investors.

#### *Options considered and preferred options*

##### **Policy issue 1: Differentiation of disclosure obligations**

10. ESMA has considered two options:

**Option 1a:** Applying the same disclosure requirements to all entities for consistency;

**Option 1b:** Reducing the mandatory disclosures depending on a de minimis threshold based on characteristics of the crypto-asset.

11. The disclosure requirements to apply to entities regarding the sustainability impacts of a crypto-asset must be justified by an increase of the investor's awareness and must be proportionate to the entity's capability to collect the necessary data.
12. ESMA considers that for crypto-assets under a certain size or that produce a smaller environmental impact, data and estimates may be less available, and disclosing entities might have fewer means to produce disclosures than larger entities. In parallel, it is likely that fewer (and in particular less specialised) investors would know of, and consider investing in, such a crypto-asset. The smaller sustainability and market impact of such a crypto-asset might therefore not warrant as extensive disclosure requirements.
13. ESMA has therefore considered both (i) on what basis to differentiate between disclosing entities and (ii) to what extent to differentiate between the requirements applicable to them.
14. First, with regards to the basis on which to differentiate them, ESMA has considered the scope of entities covered under this mandate, namely all entities obliged respectively by Titles II, III, IV and V of MiCA, and the respective costs and benefits of requiring them to produce sustainability-related disclosures provided for in this mandate.
15. ESMA has considered whether it would be appropriate to differentiate between the requirements that apply to persons producing crypto-asset white papers for asset-referenced tokens, e-money tokens, and crypto-assets other than ARTs and EMTs, respectively.
16. ESMA has also considered whether to differentiate between the requirements that apply to persons producing crypto-asset white papers within these categories, based on factors relating to the intrinsic impact of individual crypto-assets on the crypto-asset markets, such as market capitalisation, significance (in the case of ARTs and EMTs) or using factors that combine the impact of individual crypto-assets on the market and on sustainability, such as total annual energy consumption of the relevant consensus mechanism.
17. Considering that MiCA does not provide a notion of significance for crypto-assets other than ARTs and EMTs, and aims establishing consistent requirements across obliged entities, ESMA has opted to introduce a threshold on the basis of the total annual energy consumption, which therefore works as both a mandatory key indicator to be disclosed for all crypto-assets and a proxy for a de minimis threshold based on the market and sustainability-related significance of the crypto-asset.

18. Based on publicly available information on electricity consumption of the DLT linked to the most widely used crypto-assets, setting the de minimis threshold at 500,000 kWh on an annual basis for all energy consumption would capture the crypto-assets with the most significant sustainability impacts.
19. Considering the fact that DLTs' main energy use is electrical by nature, the electricity consumption is seen as a reasonable proxy for energy consumption to facilitate disclosures. The selected threshold has been identified as an appropriate way to distinguish between annual electricity consumption of the largest DLTs currently in use and that of the others.
20. Second, with regards to the extent to which to differentiate between the requirements applicable to persons disclosing information in relation to crypto-assets above or below the de minimis threshold, ESMA proposes mandatory requirements for crypto-assets for which the total annual energy consumption of the relevant consensus mechanism falls below the de minimis threshold, with supplementary mandatory disclosures in relation to crypto-assets issued by DLTs whose total annual energy consumption exceeds this threshold.
21. In turn, ESMA has considered the role, objective and costs of crypto-asset service providers' own disclosures under Article 66 of MiCA, taking into consideration the fact that Article 66(5) does not differentiate between types of crypto-asset service providers.
22. Multiple scenarios were considered, the most likely being that of crypto-assets for which a white paper already exists because it has been drafted on the basis of Title II, III or IV requirements by any of the obliged entities (including in some cases by a crypto-asset service provider operating a trading platform). In such a case the crypto-asset service provider is authorised by Article 66(5) of MiCA to retrieve from an existing crypto-asset white paper the information relevant for its own disclosures under Article 66.
23. There may also be cases where a crypto-asset service provider legitimately provides services in relation to a crypto-asset for which no crypto-asset white paper has been produced or is required. Article 4(5) provides some exceptions for which Article 66(5) may not apply, however ESMA has considered that where Article 66(5) does apply, more considerable requirements would be justified for crypto-asset service providers that are client facing and/or that directly provide opportunities for transactions, namely those operating trading platforms, those offering the exchange of crypto-assets for funds and those offering the exchange of crypto-assets for other crypto-assets, than for other types of crypto-asset service providers.
24. ESMA has therefore introduced a differentiation between types of crypto-asset service providers and the requirements that apply to them under Article 66(5) of MiCA, noting that where any of the other mandates included in this RTS apply to an entity drafting a white paper in its capacity as CASP operating a trading platform, both the requirements under Article 5 and 6 of this RTS will apply to them.

## Policy issue 2: Requirements on data collection

25. ESMA has considered two options:

**Option 2a:** Requiring all entities to rely on primary data on the consensus mechanism for the production of their sustainability disclosures;

**Option 2b:** Allowing for the use of estimates when data are shown not to be available.

26. ESMA has aimed at maintaining consistency with the requirements of existing frameworks on sustainability disclosures, including ESRS. ESMA has also considered that consensus mechanisms are generally deemed to provide more transparency, which would allow for more availability of data.

27. ESMA also acknowledges the challenges in collecting accurate data from the various network participants, especially in the first period of application of MiCA, when reliable data sources may still need to be identified. It is also expected that entities may incur costs for the collection of the data, at least until market-led solutions provide more accessible data sources. It is important that the costs are balanced with the benefits generated in terms of investor awareness.

28. Thus, ESMA has opted for the second option, introducing the ‘best effort’ clause to allow for the use of estimates when reliable data are shown not to be accessible, while requiring disclosing entities to provide information relating to their efforts and method for computing the estimates they use.

## Policy issue 3: Verification by a third-party entity

29. ESMA has considered two options:

**Option 3a:** Leaving the choice to CASPs and persons drawing up a white paper to involve a third-party for the review of sustainability disclosures;

**Option 3b:** Introducing an obligation for the verification of disclosures by a third-party entity.

30. The verification of the information through third-party entities promotes further credibility of sustainability disclosures, especially as long as common and reliable data sources have not been identified. However, this step implies additional challenges in terms of higher costs and identification of audit methodologies, which may be disproportionate considering the additional benefit in terms of reliability of disclosures.

31. Thus, ESMA has opted for the first option, leaving the choice to CASPs and persons drawing up a white paper whether to rely or not on a third-party entity for the verification of disclosures.

## *Cost-benefit analysis*

32. The draft RTS specifying the content, methodologies, and presentation of the information of the sustainability indicators of crypto-assets are expected to result in costs for CASPs and persons drawing up crypto-asset white papers, but also in benefits for investors and for environmental protection.
33. The costs described hereafter are mainly attributable to Level 1 regulation, which sets the disclosure requirements and mandates ESMA to consider on the use of energy and natural resources and on the production of waste and greenhouse gas emissions, as well as to outline key energy indicators. In the draft RTS, ESMA aimed at alleviating some of these costs through the harmonisation of the disclosure requirements, to promote economies of scale, and through the adaptation of these requirements depending on the size and volume of each crypto-asset, as prescribed by Recital (7) of MiCA.

#### *Costs*

34. Persons drawing up crypto-asset white papers are expected to incur additional costs in terms of increased use of internal resources or use of external providers for the collection of the necessary data to develop the sustainability indicators. These costs are expected to be especially high in the initial period of application of the draft RTS, when the necessary data may be less available, since a market for these data still needs to be developed.
35. Additionally, for persons drawing up crypto-asset white papers, ongoing costs would be related to monitoring of the crypto-asset and the update of the information in the white papers, at least annually.
36. CASPs are expected to incur ongoing costs due to the monitoring activities for the collection of the information and the update of their website. The monitoring will concern the white papers of the crypto-assets for which they provide services, and in some cases the websites of CASPs that provide services for the same crypto-asset.

#### *Benefits*

37. The draft RTS promote further investor awareness, adding the information on environmental impact to the criteria available to investors when comparing different crypto-assets. The harmonised application of requirements also fosters fair competition between CASPs and between persons drawing up white papers.
38. The introduction of harmonised disclosure requirements promotes fair competition between CASPs and persons drawing up white papers, while it dampens the risk of greenwashing, as all entities are required to disclose their calculation methodologies and data sources.

39. The disclosure obligation of the adverse environmental impacts of crypto-assets may push persons drawing up white papers to shift towards consensus mechanisms that have less of an impact on the environment.

*Table: Costs and benefits*

Stakeholder groups affected	Costs	Benefits
Persons drawing up crypto-asset white papers	Initial high costs related to the collection of data and/or production of estimates  Ongoing costs to keep the information in the white paper updated	Further investor awareness on the environmental impact of different crypto-assets  Incentive to use consensus mechanisms with lower sustainability impacts
CASPs	Ongoing costs for the update of the CASP's website in accordance with crypto-asset white papers and other CASPs' disclosures	Further investor awareness on the environmental impact of different crypto-assets  Prevention of green-washing practices

### 8.1.2 RTS on measures ensuring continuity and regularity of CASP services

*Impact of the draft RTS under Article 68(10)(a) of MiCA*

40. As per Article 10(1) of Regulation (EU) No 1095/2010, any draft regulatory technical standards and implementing technical standards developed by ESMA shall be accompanied by an analysis of 'the potential related costs and benefits' of the technical standards.
41. The next section presents the cost-benefit analysis of the main policy options included in this final report for the requirements for the RTS on CASP business continuity.

*Problem identification*

42. MiCA introduces governance requirements for CASPs that include a minimum set of business continuity measures that they should implement to limit the potentially harmful consequences for clients of operational disruptions that may result in service downtime or irregularities. Since CASPs will already be subject to DORA ICT business continuity

requirements, MiCA introduces requirements targeting those elements that would not fall under the scope of DORA. This would include any of the CASP's business processes or critical and important functions that do not rely on ICT systems.

43. However, some types of distributed ledgers used by CASPs in the performance of their services may be associated with elevated risks to business continuity which would not be captured under either the DORA Level 1 and Level 2 frameworks or in MiCA Level 1. In particular, permissionless DLTs with limited interoperability vis-à-vis other DLTs and hence no options for back-up and recovery procedures represent one source of elevated risk.
44. Clients of CASPs (both individual investors or other financial entities) are therefore subjected to this operational risk downstream of the services relying on permissionless DLT with few options for recourse or methods of risk mitigation available to them. In most cases, end-clients understand this distinct feature of the crypto market and accept it as an idiosyncratic risk in a trade-off with the benefits of atomic settlement and trustless transactions.

#### *Policy objectives*

45. The strategic objective of this draft RTS is to ensure CASPs have adequate governance arrangements in place to mitigate circumstances that would threaten the regularity or continuity of their services, and, in the scenario of a service downtime, effectively resume services within their established recovery time and recovery point objectives.
46. In light of this objective, the draft RTS acknowledges that despite the elevated risks to business continuity associated with permissionless DLTs, there are certain compensatory measures CASPs can implement in their business continuity plans to limit the adverse effects for clients of a cessation or degradation of services.

#### *Baseline scenario*

47. In the baseline scenario, CASPs would be subject to the relevant governance obligations outlined in Article 68 of MiCA with no specification of how they should implement and comply with those measures. Further, in the absence of this RTS, CASPs and their clients would have no indication of how permissionless DLT should be treated for the purposes of business continuity.
48. The result of this would be disparity in the levels of rigour of compliance with the business continuity requirements among CASPs. As such, the quality of recovery from an operational disruption may vary drastically from one CASP to the next—with consequences for investor protection. Compounding this disparity in the application of these business continuity measures, in the absence of a standardised self-assessment, there would be no baseline or reference point with which NCAs may assess the riskiness of a CASP's business model and the impact a disruption to their services may have on the wider crypto market.



### *Options considered and preferred options*

#### Policy issue 1: Organisational arrangements for effective implementation of CASP business continuity measures

49. ESMA considered two policy options:

**Option 1a:** Require CASPs to establish a dedicated business continuity management function at the level of the senior management to oversee the business continuity policy and the obligations set out in the draft RTS.

**Option 1b:** Allow CASPs to use existing resources and functions for the governance of business continuity management, provided such existing resources are sufficient for the adequate implementation of the general business continuity policy.

50. ESMA selected option 1b. Given the narrow mandate for defining organisational arrangements of the CASP in Level 1, it is difficult for ESMA to justify a more intensive set of governance obligations.

### *Costs*

51. No additional costs for CASPs, NCAs or clients of CASPs.

### *Benefits*

52. Allowing CASPs to share resources and functions with an existing function at the level of their senior management which is already dedicated to risk management would alleviate the burden of dedicating staff to a purpose whose value-added is questionable given the redundancy it would entail. For example, CASPs may designate the same control function required under Article 6(4) of Regulation (EU) 2022/2554 as competent for the non-ICT (or 'general') business continuity requirements of this RTS. This would be a natural fit considering the overlap between the DORA and MiCA regimes as it relates to business continuity measures.

#### Policy issue 2: Business continuity measures for permissionless DLT

53. ESMA considered three policy options:

**Option 2a:** Stay silent about the regulatory treatment of permissionless DLT and allow CASPs to address the associated business continuity risks in a manner they deem sufficient.

**Option 2b:** Provide regulatory guidance specific to the measures CASPs should take to incorporate the use of permissionless DLT into their business continuity policies and plans.

**Option 2c:** Treat permissionless DLT as an ‘ICT service’ or a ‘critical or important function’<sup>26</sup> of the CASP and hence subject to strict business continuity requirements such as back-up and recovery procedures found in DORA and other relevant sectoral regulations for ICT risk management.

54. ESMA has selected option 2b. By addressing the specific risks posed by permissionless DLT in the draft RTS, we provide clarity around their expected regulatory treatment by supervising NCAs.

#### *Costs*

55. This is a new obligation not derived from Level 1 and hence could impose additional compliance costs on CASPs. However, as CASPs would already be subject to an equivalent provision for external communications in Article 14 of Regulation (EU) 2022/2554 as it relates to ICT incidents, this may defray some of the costs of maintaining staff or resources in charge of client communications for the purposes of MiCA requirements. In any case, regular communication with clients already constitutes an industry best practice and CASPs would likely find themselves implementing this voluntarily in the absence of the provision due to competitive pressures.

#### *Benefits*

56. The benefits would include ongoing communication from CASPs to their clients in the scenario of a disruption, including regular updates about the status of their affected services and whether their funds are compromised. Access to timely information about the status of their funds or services would enable clients to, for instance, trigger insurance claims or other risk mitigation measures.

#### **Policy issue 3: Proportionality and risk considerations**

57. ESMA considered two policy options:

**Option 3a:** Require a self-assessment to support competent authorities in their assessments of proportionality considerations in supervision of business continuity measures.

**Option 3b:** No self-assessment. CASPs and their supervisors use their own indicators to determine the scale, risk and complexity of the organisation and hence the business continuity measures commensurate with those indicators.

---

<sup>26</sup> See definitions of ‘ICT services’ and ‘critical or important functions’ in Article 3, paragraphs 21 and 22 of Regulation (EU) 2022/2554 (DORA)

58. ESMA has selected option 3a to require a self-assessment (in Article 6(2) of the draft RTS), which is intended to supplement the competent authority’s risk-based supervision of a CASP business continuity measures.

#### Costs

59. The self-assessment would require CASPs to annually review their operations, taking stock of a range of metrics on their users, assets offered, and ICT infrastructure deployed in their services. This would impose marginal compliance burdens on the CASP. It should be noted that none of the metrics required in the assessment would require rigorous accounting or forensic data analysis. Indeed, many of the data points may already be tracked by CASPs as part of their KPIs for business performance purposes.

#### Benefits

60. Upon request, NCAs will be capable of verifying the results of a CASP’s self-assessment to understand if their business continuity measures are commensurate with the risks associated with their scale and complexity. It would enable to use a data-driven approach to risk-based supervision with due consideration for proportionality.

Table: Costs and benefits of the draft RTS on CASP business continuity

Stakeholder groups affected	Costs	Benefits
CASPs	<p>Ongoing compliance costs to prepare the business continuity policy, test its implementation, and review on an annual basis. (<i>Note: these costs originate from Level 1 obligations</i>)</p> <p>Ongoing compliance costs to prepare the self-assessment.</p>	<p>1) The ability to use the existing functions at the level of their senior management (including those required for ICT risk management under DORA) to fulfil the business continuity governance obligations in the draft RTS.</p> <p>2) Clarity on how permissionless DLT would be treated under the regulatory framework for business continuity measures.</p> <p>3) With the self-assessment, CASPs benefit indirectly because NCAs will have a tool with which to determine adequate risk-based supervision measures commensurate with the risks posed by a CASP.</p>

Stakeholder groups affected	Costs	Benefits
Competent authorities	Ongoing costs to supervise compliance with business continuity measures. <i>(Note: these costs originate from Level 1 obligations)</i>	With the inclusion of a CASP self-assessment on risk considerations, competent authorities will have access to a set of standardised metrics with which to assess relative risks between CASPs and implement proportionality into their ongoing supervision.
Clients of CASPs	N/A	Added protections afforded by 'timely communications' from CASPs in the event of a disruption to services involving a permissionless DLT.

### 8.1.3 RTS on trade transparency

#### *Impact of the draft RTS under Article 76(16)(a) of MiCA*

61. As per Article 10(1) of Regulation (EU) No 1095/2010, any draft regulatory technical standards (RTS) developed by ESMA are to be accompanied by an analysis of “the potential related costs and benefits” of the technical standards, unless such analyses “are highly disproportionate in relation to the scope and impact of the draft regulatory technical standards concerned or in relation to the particular urgency of the matter”.
62. The following section outlines ESMA’s assessment of the main policies included in the draft RTS further specifying the manner in which transparency data, including the level of disaggregation of the data to be made available to the public, is to be presented.

#### *Problem identification*

63. Transparency is paramount to well-functioning of markets. It is often described as an inherent feature of trading platforms for crypto-assets and, more broadly, of the Distributed Ledger Technology (DLT) where, in particular in the case of public distributed ledgers or blockchains, all relevant data and transactions are, once verified, recorded in chained blocks and therefore made available to everyone. Transparency is commonly described as a broadly accepted market practice for trading platforms in crypto-assets.
64. Nevertheless, the absence of this draft RTS would entail that each trading platform publishes the information under their own standards and content. It would not create an environment where users of data would be able to quickly, easily, and accurately analyse or compare data points from different trading platforms in order to arrive at the best investment decision. This would also make the aggregation of data very challenging and costly preventing market participants from having a holistic view on crypto-asset markets.

65. The lack of standardised information would have an adverse impact on crypto-assets markets and hinder the level playing field between sophisticated investors, who could easily build systems to make information comparable, and retail investors. Therefore, MiCA creates the obligation for trading platforms to publish pre-and post-trade information whilst tasking ESMA to develop an RTS to further specify how this information should be presented.

#### *Policy objectives*

66. The objective of this draft RTS is to enhance pre- and post-trade transparency available to investors. The RTS further specifies the information that have to be made available to the public and sets out the data fields and standards that should be followed when publishing transparency information. In addition, the draft RTS ensures that the operating rules used by trading platforms for crypto-assets are transparent.
67. Finally, the draft RTS includes the level of data disaggregation that should be made available to the public so that data users can customise their data solutions to the furthest possible degree to ensure that consumers only pay for the real-time data they need.

#### *Baseline scenario*

68. ESMA notes that MiCA (level 1) already envisages a certain degree of standardisation and convergence regarding the information to be made public by trading platforms for crypto-assets. More specifically:
- i. Article 76(9) sets out that trading platforms for crypto-assets “*shall make public any bid and ask prices and the depth of trading interests at those prices which are advertised for crypto-assets through their trading platforms [and] make that information available to the public on a continuous basis during trading hours*”.
  - ii. Article 76(10) sets out that trading platforms for crypto-assets “*shall make public the price, volume and time of the transactions executed in respect of crypto-assets traded on their trading platforms [and] make those details for all such transactions public as close to real-time as is technically possible*”.
  - iii. In addition, Article 76(16)(a) of MiCA requires ESMA to specify “*the manner in which transparency data, including the level of disaggregation of the data to be made available to the public*”. Through this mandate, co-legislators have already envisaged within MiCA not only new disclosure requirements but also a common disclosing “*manner*”.
69. Therefore, the impact of the draft RTS is rather on the degree of standardisation for the transparency disclosures that will be required from trading platform for crypto-assets. Where the final draft RTS creates additional obligations, the costs associated with the incremental rule will be a combination of the effects of the Level 1 text and of the final draft RTS. As those effects are very difficult to disentangle, any indication of costs is to be considered as an upper bound.
70. In addition, regarding the specific format of the information to be disclosed for the purposes of pre- and post-trade transparency, ESMA aligned the requirements of its draft

RTS with the requirements established within the draft RTS on record-keeping. The costs attached to such formats have therefore been assessed in the cost and benefit analysis of the draft RTS on record-keeping.

#### *Options considered and cost-benefit analysis*

71. This section presents the main policy options discussed and the decisions made when developing the draft RTS. The advantages and disadvantages of each policy options and the cost-benefit analysis resulting from the assessment are evaluated below.

#### **Policy issue 1: Pre-trade information to be published by trading platforms operated by CASPs**

72. ESMA considered two policy options on how pre-trade information should be published:

**Option 1a:** Build on the existing pre-trade transparency regime for traditional financial instruments embedded in MiFIR and include high level requirements on which information should be made available to the public.

**Option 1b:** Create a standardised regime setting out the data fields that need to be published for the purpose of pre-trade transparency.

73. The calibration of the information to be provided for the purpose of pre-trade transparency via high-level requirements would already improve the information available to stakeholders. However, ESMA considered that further aligning practices on the exact information to be provided would ensure that stakeholders would have the same content and format across trading platforms when accessing pre-trade data. If Option 1b represents higher compliance costs for trading platforms for crypto-assets, it also reduces costs for data users to consume the published data ensuring easier and faster comparability and aggregation of the information leading ultimately to more informed investment decisions.
74. In addition, ESMA notes that even under Option 1a, the new MiCA requirements, by prescribing specific disclosure details (i.e., “make public any bid and ask prices and the depth of trading interests at those prices which are advertised for crypto-assets [...] on a continuous basis”), would have in certain cases imply adjustments to the disclosure arrangements currently used by trading platforms. Therefore, Option 1a would have also led to one-off and on-going compliance costs for these trading venues but without bringing clear benefits to data users.
75. Finally, the standardised disclosure regime under Option 1b would allow further calibration of the information disclosed allowing in certain cases more targeted disclosure (e.g. disclosure limited to the five best bid and offer price levels for a CLOB).
76. Thus, ESMA considered that the benefits that enhanced standardisation of pre-trade information would represent for data users far outweighs the costs that such standardisation implies for trading platforms for crypto-assets who will have to update their systems. Therefore, Option 1b was chosen as the preferred option.

### Policy issue 2: Approach to reserve and other orders (such as stop loss orders, once-cancels-the-other-orders)

77. ESMA considered two policy options on how to address the absence of pre-trade transparency waivers:

**Option 2a:** no exemption for any type of orders in the absence of waivers in MiCA, meaning that some order types would not be available for trading platforms.

**Option 2b:** narrowly define some type of orders that meet certain requirements that can be offered by trading platforms without undermining pre-trade transparency disclosures.

78. MiCA does not provide for any exemption to pre- and post-trade transparency and ESMA cannot create any exemption to pre-trade transparency in the RTS, as it lies outside the scope of the mandate.

79. Nevertheless, reserve orders and, for example stop loss orders, can be regarded as risk management tools which can benefit retail investors. By removing the possibility of trading platforms to offer these orders, market participants would still be able to develop these strategies using their own order management facilities. However, the development of an order management facility requires substantial technical and financial resources and would therefore not be available for retail investors putting them at a competitive disadvantage.

80. In addition, it should be noted that the objective of allowing trading platforms to offer embedded order management facilities is to provide investors with ready-made tools to facilitate the execution of their orders and strategies, allowing for instance to reduce the price impact of large orders and to automatically frame a trading strategy and protect the investor from unexpected price movements. Furthermore, for financial instruments under MiFIR the objective of requiring trading venues to request a waiver for those types of orders was to better monitor the use of these specific order types.

81. Neither option would require significant costs for trading platforms as offering these types of orders are already offered to users in most cases and, for the cases where trading platforms do not offer these trading functionalities, the draft RTS does not impose any obligations to develop any systems and hence no further costs would be imposed on trading platforms.

82. Therefore, ESMA is of the view that the draft RTS should calibrate the pre-trade transparency regime for crypto-assets so that orders which meet the three narrowly defined conditions, can be offered by trading platforms. Thus, Option 2b was chosen as the preferred option.

### Policy issue 3: Data fields to be published by trading platforms operated by CASPs for the purposes of post-trade information

83. ESMA considered two policy option on which type of trading fields and formats should be published by CASPs:



**Option 3a:** Leverage on the information required to be published for traditional financial instruments embedded in MiFIR, by adapting some fields and format to the reality of crypto-assets.

**Option 3b:** Create a standalone regime for the purposes of crypto-asset trading with new fields and formats created for this purpose.

84. In the same way as for pre-trade transparency requirements, the calibration of the information to be provided adds costs for trading platforms, both one-off costs to develop the publication tools and compliance costs related to operational expenses for data collection, analysis, and reporting. CASPs operating a trading platform would need to allocate resources for monitoring and ensuring compliant levels of data quality. ESMA aimed at alleviating some of these costs through the harmonisation of the requirements, by using requirements already set out for traditional finance, whilst at the same time adjusting these requirements to the specificities of crypto-assets.
85. However, despite trading platforms operated by CASPs are expected to increase their costs it on the other hand benefits investors and data users. The harmonised data fields to be published improves the trade data information disclosed and ensures that practices for disclosing information are aligned thereby allowing investors and data users to have the same information available regardless of the trading platform they use.
86. When assessing which data fields to be published, this draft RTS leverages on the work performed on the RTS for record-keeping in order to align the data fields as much as possible and ensuring that only essential information related to the trading of crypto-assets is required. Hence, the specific cost and benefit analysis on the fields to be published are assessed in the context of the record-keeping RTS. This solution would reduce the costs for trading platforms, as they would only have to develop one solution for data collection. Despite having ongoing operational expenses related to data collection, analysis, and reporting, the initial cost would be lower than if a different solution were selected. Whilst CASPs operating a trading platform need to allocate resources for monitoring and ensuring compliance of data quality, the standardisation promotes further investor awareness, adding information available to investors. Thus, considering the costs and benefits, ESMA opted for Option 3a.

#### Policy issue 4: definition of “as close to real-time as is technically possible”

87. ESMA considered three policy options when considering the meaning of “*as close to real-time as is technically possible*”.

**Option 4a:** not defining the concept of real-time and allowing trading platforms to set out their own time limits for the publication of transactions.

**Option 4b:** Aligning the requirement to that applicable to traditional finance prescribed in MiFIR, in particular equity instruments.

**Option 4c:** Define the concept of “as close to real-time as is technically possible” in line with the technical capabilities embedded in crypto asset trading environment.

88. In the context of financial instruments under MiFIR, trading venues are required to publish post-trade information as close to real-time as is technically possible and in any case within one minute for equity instruments. Considering the technical capabilities and speed of execution within crypto-asset markets, post-trade transparency should be published immediately after execution. Information should be made available instantaneously after execution and only in exceptional circumstances should publication occur within a fixed period of time after execution. To cater for those exceptions, the draft RTS allows for a short period, of thirty seconds, to still be considered real-time.
89. The clear definition of the concept of ‘real-time’ benefits investors as it gives them a clear expectation of when a trade should be published. Considering the speed of execution and the technical capabilities of trading platforms, a shorter period than that available for equity instruments is envisaged for crypto-assets.
90. ESMA considers that the definition embedded in the draft RTS does not increase costs for trading platforms as the investments to ensure a publication real-time is embedded in Level 1 and the draft RTS simply clarifies the maximum leeway. Thus, Option 4c was chosen as the preferred option.

*Table: Costs and benefits*

<b>Stakeholder groups affected</b>	<b>Costs</b>	<b>Benefits</b>
<b>CASPs</b>	<p>One-off costs for the development of systems to ensure pre-trade information is published on a real-time basis in a standardised manner.</p> <p>Ongoing costs for operational expenses related to data collection, analysis, and reporting. CASPs operating a trading platform need to allocate resources for monitoring, and ensuring compliance of data quality.</p> <p>Compliance with transparency requirements might necessitate changes to existing trading platforms, potentially increasing operational overhead for crypto trading platforms.</p>	<p>Clarity on data standards and publication arrangements for transparency data.</p> <p>Ability to offer reserve and other types of others increases risk management tools offered to users and therefore attracts further investors.</p>

Stakeholder groups affected	Costs	Benefits
	Ongoing costs for website maintenance in as necessary, i.e., when the operating rules published on the website of crypto-asset trading platform are revised.	
Investors and data users	One-off costs for the development of systems to ensure they can aggregate all information available across the market.	<p>Promotes further investor awareness on trade data.</p> <p>Disclosure of pre- and post-trade data information in a standardised manner ensures that investors and data users have the same information available regardless of the trading platform they use.</p> <p>Ability to make use of risk management tools, such as reserve orders, for the trading activity.</p> <p>Availability of operating rules in an easy, fair and simple manner.</p> <p>Only purchase data they consume.</p>

### 8.1.4 RTS on record-keeping by crypto-asset service providers

#### *Problem identification*

91. MiCA introduces new record-keeping obligations for CASPs. Given the novelty of the crypto-asset markets, it's crucial for CASPs to understand what data should be reported and in which format. Without a common format, there could be a variety of different formats, which could impose an unnecessary burden on CASPs.
92. Further, National Competent Authorities (NCAs) are tasked with duties pertaining to investor protection, market monitoring, and market abuse surveillance of the crypto-asset market. To effectively detect potential market abuse or illegal activities, it is crucial that they receive accurate and comprehensive information on transactions and orders.
93. In order to streamline the reporting process, reduce the CASPs compliance burden that would stem from several local data requirements and enable data driven monitoring of

NCA, it is necessary for CASPs to report the data in a standardised format and consistent manner. Additionally, all the parties involved in the crypto-asset transactions and the crypto asset being traded need to be uniquely and consistently identified in a fully automated manner. These elements are the pre-condition for supervisors to be able to monitor the orderly functioning of the crypto assets markets and thus build investors' trust. This is especially relevant for crypto markets where supervisors need to adapt their supervisory efforts and tools with the pace of technological and financial innovation.

#### *Policy objectives*

94. The purpose of Article 68(9) and (10)(b) is to specify the records that the CASPs are required to maintain in order for the national competent authorities to fulfil their supervisory task in order to protect the investors and the market. To enable the national competent authorities to identify market abuse, the record keeping by CAPS must be kept at a granular level and in a common format, both at the order and transaction level.
95. In accordance with Article 94(1)(a) of MiCA, NCAs have the power to require any information they consider as possibly relevant for the performance of their duties. This provision is to be read in conjunction with the above-mentioned provisions regarding record keeping obligation functional to NCAs' fulfilment of their supervisory and market integrity tasks.

#### *Baseline scenario*

96. In the absence of these technical standards, the crypto-assets service providers would be subject to the obligation to record all the information related to orders and transactions without specification as to which are the relevant details to be recorded as well as the appropriate format in which order-book information should be provided to regulators. The result of this would be disparity in the levels of rigour of compliance across CASPs, exposing them to different request for data by the various national competent authorities to be provided in different formats depending on the national preference. Ultimately this increases the costs of compliance and results in lack of comparability of order and transaction information to be recorded by different CASPs in different member states.

#### *Policy options and preferred options*

97. The next paragraphs present the cost-benefit analysis of the main policy options regarding the format of the records, the identifiers to be used for parties and crypto assets and the on-chain specific data elements. The various policy options, and their respective advantages and disadvantages are assessed below, where ESMA has also identified the preferred options resulting from this analysis.
98. ESMA assessed that the incremental costs stemming from the preferred options on these aspects are minimal. However, to further mitigate the costs, ESMA plans to acquire a common solution for the monitoring of crypto markets to ensure that costs are mutualised and to facilitate supervision of cross-border market activities. This approach

will reduce IT and compliance costs for both CASPs and supervisory authorities. A key component of the common solution is the reliance on the reference data on crypto assets maintained by the Digital Token Identifier Foundation, which ensures consistent identification of the crypto asset traded across multiple platforms, CASPs and blockchains.

#### Policy issue 1: Format of the record-keeping by CASPs

99. The requirements proposed by ESMA for the record keeping by CASPs builds upon existing legislative frameworks such as those established under MiFIR/MiFID II. In this context, several format options were considered and the most suitable format for supervisory data was selected. Concerning the format in which the information should be provided to the national competent authorities, to avoid duplicative requirements and additional burden, ESMA considered that once requested by the authority, the records should be provided in the same format as the one prescribed for the order-book records. For a detailed analysis on the format options, please refer to the next section on the formats to be used for the maintenance of order-book records. Nevertheless, ESMA acknowledges the distinct differences between traditional financial instruments under MiFID II and crypto-assets under MiCA. Therefore, ESMA has tailored the draft RTS to minimise the implementation burden while considering the disparities.

#### *Costs*

100. Given the legal framework and the need for the CASP to deliver the information to the competent authority and considering that, in order for it to be processed by the authority, the information must be delivered in a certain format, ESMA TS prescribe the specific format in which the information should be delivered. This approach reduces the burden of compliance as it ensures that the CASP do not need to convert the information into multiple formats when requested by different national competent authorities. ESMA considers that this approach strikes the right balance between the surveillance needs of national competent authorities to have standardised transaction data that is comparable with order data while permitting CASPs to maintain their own internal databases with relevant mapping tables and without any loss of original raw data. Additional analysis of the costs arising from the specific format chosen for both transactions and order data to be provided by Crypto Assets Service Providers are provided in the next section of this CBA on the order-book records to be maintained by trading platforms.

#### *Benefits*

101. The proposed RTS enables ESMA to fulfil its mandate while reducing impact on CASPs and maintaining a technology-neutral approach. Given the need to automatically process the data that must be kept, as well as the novelty of the crypto-asset industry, the CASPs that are not yet operating in traditional financial markets will need to implement one-off IT processes to provide the record-kept data in the requested format. However, ESMA's proposal, which takes into consideration other existing regulations, enables ESMA to reduce the burden for CASPs by relying on trusted format, widely adopted across the

industry. It also allows CASPs to have a reduced implementation cost, by keeping the information in other formats and only needing for a conversion whenever a national competent authorities request such data.

102. Without a common format, national competent authorities face the limitations of not having harmonized information readily available, as well as a lack of format standardization. The lack of format standardization in turn makes market surveillance activities by national competent authorities extremely difficult, especially in the case of cross-venue operations on the same crypto asset.
103. The use of a common format presents several benefits stemming from the application of some of the objectives of the Strategy on supervisory data for Financial Services<sup>27</sup>. First of all, the record-keeping of the information in a standardized format will allow for data to be retrieved by NCAs to be better compared across all other data stemming from existing reporting systems. This is more broadly aligned with ESMA's efforts to ensure the comparability and compatibility of available data to national competent authorities across different regimes.
104. Secondly, the use of a common format across reporting regimes allows for enhanced data-sharing across authorities and better market monitoring of the activity of CASPs. This in turn will allow NCAs to better detect and assess potential market manipulation and other fraudulent behaviours conducted through several market members trading in crypto-assets.
105. Thirdly, a high degree of standardization of formats can have significant benefits for national competent authorities arising from better efficiencies and lower costs of any surveillance or market monitoring tools developed by national competent authorities or that include several authorities concurrently. The more standardized the data retrieved by national competent authorities is, the lower the cost of processing the data made available by CASPs will be.

#### Policy issue 2: Legal Entity Identifiers related to clients/buyers/sellers

106. Technological innovations will continue to change the way financial products are being designed and distributed. The collapse of the crypto-currency exchange, FTX, underlined the urgency of consistent application and supervision of trading in crypto assets across the EU. Identifying in a timely manner, through the use of data-driven tools, the activities of participants in crypto assets markets and their group structure is key to support a risk-based, pro-active and outcome-focused supervision. To achieve this, the clients, buyers, and sellers participating in these markets must be identifiable in a unique and consistent manner via an identification system that enables fully automated and timely retrieval of the basic information on these entities in all legs of the transaction chain. Therefore,

---

<sup>27</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0798>



ESMA proposes that if the clients/buyers/sellers are eligible for a Legal Entity Identifiers (LEI), they should be identified by it.

## Costs

### *Costs for parties involved in crypto transactions*

107. The main cost related to the identification of legal entities is that LEI is a paid identifier and entails some costs on the entities who do not already have one and must obtain it. The average LEI registration fee in Europe is approximately EUR 60. However, all clients of financial institutions participating in financial instruments transactions already have an LEI therefore there is no further costs for such clients. ESMA estimates indicate that the number of unique buyer/sellers with an LEI reported under EMIR and MiFIR requirements over the last year ranges between 450-550 thousand entities. So, there is no extra costs for these entities already trading in Europe to use the LEI in MiCA. Based on the EMIR and MiFIR data as of today and the information exchange with the stakeholder's vendor group of the global LEI system<sup>28</sup>, ESMA estimates that, as a minimum, 70% of these LEIs are already assigned to non-financial firms. Recent statistics<sup>29</sup> indicate that a significant proportion of trading in digital assets is expected to continue alongside trading in financial instrument. ESMA expects that the new buyers/sellers that are currently not engaging in EU financial markets will mostly be represented by individual natural persons<sup>30</sup> for which these technical standards prescribe a separate free of charge identification method.
108. For clients who do not currently engage in EU financial markets that are legal entities, financial Institutions and crypto assets services providers can obtain LEIs for their clients through the Validation Agent model<sup>31</sup>. This model was used by several financial institutions to ensure compliance with EMIR and MiFIR requirements and ensures that the acquisition of the LEI code for the clients is embedded in the standard account opening process. Currently there are 19 Validation Agents in the Global LEI System including major global banks like BNP Paribas, JP Morgan, Citibank, and Goldman Sachs.
109. While LEI may entail some costs for the buying/selling parties, consolidated access to the full set of LEI reference data is free of charge for the users, retail investors, market participants and regulators. Today, the financial institutions that service parties to financial instruments transactions use the LEI as a source for the basic customer information meaning free and automated access to the basic customer information data for their own internal operations.

---

<sup>28</sup> [GLEIF stakeholder group](#)

<sup>29</sup> <https://www.treasurers.org/hub/blog/insights-digital-assets-survey-2024>

<sup>30</sup> Examples of small individual investors involved in crypto markets: <https://www.cnn.com/2023/10/02/ftx-customers-who-lost-fortune-are-doubling-down-on-crypto.html>; <https://www.entrepreneur.com/business-news/who-lost-money-in-ftx-tom-brady-kevin-oleary-and-more/443653>

<sup>31</sup> [Validation Agents - Solutions – GLEIF](#)



### *Costs for supervisors and supervised entities*

110. EU regulators have already embedded the LEI in their systems, there will be no additional cost associated. Overall speaking, the LEI is a no cost solution for financial supervisors. This helps reducing the burden on the supervised entities as well because it means that there will be no increase in supervisory fees charged by the market supervisors to fund their activities.
111. According to an estimation conducted ZEW, a cost-efficient European supervisory framework (proxied by supervisory cost) could save up to 15% institutional cost<sup>32</sup>, and the annual supervisory cost from the ECB alone is over 650 million euro<sup>33</sup>. The annual supervisory cost of other supervision bodies varies from 10 million euro to 700 million euro with an average of 200 million euro in 2013, and the overall trend is still increasing over time<sup>34</sup>.

### *Benefits*

112. The main benefits of using the LEI for identification of client/buyer/seller is that LEI is a global identifier, which is already used among the supervisors. For instance, all current national market surveillance systems as well as the databases that ESMA runs at EU level are wired to the LEI code and can easily interact with each other. This is because the LEI code act as common key to ensure that data from different sources can be linked, validated, and exchanged. For the surveillance purpose, the availability of a central database (GLEIF) where many separate data elements characterising the legal entity are maintained in a standardised manner, following strict data quality protocols, and allowing daily downloads of its full content is key for these purposes. Finally, as the LEI is already required for participants in traditional financial markets, the extension of this requirement to participants in crypto markets will enable the market supervisors to monitor the trading activity of the same entity engaging in both traditional and crypto markets. So far, the market supervisors are not aware of any other alternative identifier that would achieve the same benefits. However, the text in the technical standards leaves the door open to alternative identifiers for non-financial entities that may not already have an LEI, should any alternative be deemed as fulfilling the same criteria as the LEI in the future.

### **Policy issue 3: Additional on-chain specific data elements**

113. Lastly, leveraging on the results from the independent study<sup>35</sup> related to the DLT Pilot Regime, ESMA propose to add on-chain specific data elements (for example, transaction hash, Gas Fee, Token ID, Wallet addresses) as its deemed relevant for the purpose of

---

<sup>32</sup> <https://ftp.zew.de/pub/zew-docs/dp/dp0501.pdf>

<sup>33</sup> <https://www.bankingsupervision.europa.eu/organisation/fees/total/html/index.en.html>

<sup>34</sup> <https://iris.luiss.it/retrieve/e163de42-2581-19c7-e053-6605fe0a8397/Costs-and-Benefits-of-Financial-Regulation.pdf>

<sup>35</sup> [ESMA12-2121844265-3183 Report on the DLT Pilot Regime - Study on transaction reporting based on RTS 22 \(europa.eu\)](#)

supervising on-chain trading activities. ESMA proposed to use the DTI for identification of crypto-asset and the transaction hash to identify transactions executed on-chain.

#### *Costs for CASPs*

114. Adding additional data fields related to the on-chain data elements will ensure that national competent authorities can tailor their requests for access to the blockchain data to a subset of data elements, which reduces the burden compared to exposing the CASPs to requests for the full blockchain data related to a given transaction.
115. When it comes to the implementation costs to the CASPs, and as described in the study on the extraction of transaction data <sup>36</sup>, it is worth noting that the extraction of the additional on-chain data fields will not represent a cost for the CASP that is comparable to the introduction of other new fields. Due to the nature of the blockchain, accessing on-chain data directly will allow the regulators real-time availability, data integrity, as well as creating a major operational efficiency for CASPs.
116. From the perspective of implementation costs for CASPs it will certainly represent a lower effort since the extraction of this subset of data will be able to happen directly. Whether this is data based or through an API, direct access to the information by the national competent authorities as well as the data integrity associated with information on-chain will compensate the implementation costs.
117. Concerning the costs arising from the use of a standard identification method for the crypto-asset (DTI), please refer to section 8.1.7 of the CBA.

#### *Costs for supervisors*

118. While it is likely that there will be costs associated with the initial setup of the solution for the regulators to access this subset of data directly on-chain, the advantages related to later access to that information by the national competent authorities without the need for communication with the CASPs via other systems, largely supersede those.

#### *Benefits*

119. The best example of a field included in the on-chain data requirements is the inclusion of the Digital Token Identifier (DTI). The DTI has been proven as the most appropriate identifier since it follows the principles of uniqueness, neutrality, reliability, open source, scalability, accessibility on a cost-recovery basis, is offered under an appropriate governance framework and is adopted for use in the Union. The main benefits are that DTI is defined by the International Organisation for Standardisation's ISO 24165 and offers linkage across the asset level (ISIN), Token level and DLT level. In addition, plans are ongoing to ensure a linkage with the LEI of the issuer of the token. An additional

---

<sup>36</sup> [ESMA12-2121844265-3182 Report on the DLT Pilot Regime – Study on the extraction of transaction data \(europa.eu\)](#)

benefit is that the DTI can also be used to report the quantity and price of transactions denominated in crypto-assets.

120. ESMA received overwhelming support to using DTI as the unique identifier (see Section 6.2.3). However, among the few respondents not supporting the proposal of using the DTI, a few said that it would cause additional burden for smaller players especially since the adoption is not broad enough yet. However, this burden on smaller players would exist for any other identifier as well given they have a weaker (if any) adoption level and it is expected that if the DTI is mandated as the unique identifier, this cost would eventually be reduced. Furthermore, no strong alternative to the DTI currently exists. Indeed, using ISIN/FIGI or token addresses/contracts do not allow for standardized identification across different blockchains, are not defined by ISO standards and are proprietary.
121. The DTI is, so far, the only standard as defined at the Union level which is a) unique; b) neutral; c) reliable; d) open source; e) scalable; f) accessible; g) available at a reasonable cost; and h) subject to an appropriate governance framework. The only alternative mentioned (by one respondent) in response to ESMA's consultation, the FIGI, does not meet the criteria of a) uniqueness, g) availability at a reasonable cost, and h) appropriate governance. Indeed, the FIGI does not allow users to identify crypto assets below the asset level (i.e., on different DLTs) free of charge. This means that in order to meet the MiCA granularity requirements, charges will apply and, given that FIGI is a proprietary identifier as it owned and governed by a private company, such charges will not be applied on a cost recovery basis.
122. When it comes to the benefits of the inclusion of the other additional on-chain data fields, ESMA has analysed these in the context of the study on DLT Pilot, the existing practices in Member States and the responses to the consultation.
123. First of all, the study provided very useful insights on the included additional data elements and their usefulness for NCAs to monitor market conduct on crypto assets trading. The study identified a number of fields, as not only relevant for the purposes of supervising on-chain trading activities under MiCA, but also as necessary for the proper cross-referencing of transactions across different crypto assets. Furthermore, ESMA considered the experience gathered by national competent authorities in monitoring on-chain trading activity under the applicable national legislation. This experience with practical applications of similar on-chain data required fields, signalled the necessity of the proposed additional fields in order for national competent authorities to properly exercise their market monitoring activities. The fact that the information is accessed on-chain, also brings the benefit of its integrity and real time access as previously described.
124. When comparing the requirements for national competent authorities to be able to properly exercise their market monitoring activities under MiCA, the study identified several differences between the requirements in RTS 22 and the ones that should be imposed in the context of MiCA. As such, several fields, derived from the DLT transaction

flows, and specified in the Smart Contract between the participants were included in the proposed recordkeeping RTS. The inclusion of additional fields allows national competent authorities to be able to access to information necessary for the proper identification of transactions happening on-chain. Some of these fields, such as the transaction hash, enable the unique identification of a transaction happening in the network, while fields such as “gas fees” or “gas limit” allow national competent authorities to retrieve additional information uniquely occurring within transactions happening within certain blockchains.

### Conclusions

125. Considering the wide-ranging support expressed in the Consultation Paper and the innovative nature of the crypto-asset markets, the advantages of employing DTI and LEI to identify market participants and crypto-assets surpass the potential costs. Given the obligations arising from Level 1, the record-keeping of CASPs must be sufficiently detailed to enable national competent authorities to carry out their surveillance duties. ESMA’s proposal for CASPs’ record-keeping takes into account the already established international standards, while adapting them to a new market in an effort to minimise the burden on market participants as much as possible. So far, the market supervisors are not aware of any other alternative identifier that would achieve the same benefits as the DTI. However, the text in the technical standards leaves the door open to alternative identifiers should any alternative be deemed as fulfilling the same criteria as the DTI in the future.

Table: Costs and benefits

Stakeholder groups affected	Costs	Benefits
CASPs	The incremental costs relating to the use of data standards are minimal considering that specific systems will need to be set up to implement the L1 requirement for CASPs to share a common set of data with NCAs.	Reducing the burden on CASPs by leveraging on already established international standards to gather crypto-assets/legal entities’ reference data and limiting costs related to NCA supervisory fees. In the case of LEI, this code is already used in Europe for trading in traditional financial instruments.
Competent authorities	Costs associated with the initial setup of the solution for the regulators to access the relevant data are stemming from the L1	LEI is a global identifier, which is already used among the supervisors LEI code act as common key to ensure

Stakeholder groups affected	Costs	Benefits
	<p>requirements. EU regulators have already embedded the LEI in their systems, there will be no additional cost associated.</p>	<p>that data from different sources can be linked, validated, and exchanged.</p> <p>The use of the same standard that is already used in Europe for identification of entities participating in traditional financial markets facilitates supervision of the activity of the same entity across crypto assets markets and traditional ones.</p> <p>DTI is defined by the International Organisation for Standardisation's ISO 24165 and offers linkage across the asset level (ISIN), Token level and DLT level.</p> <p>Direct and automated access to good quality information through standardized central registries (GLEIF and DTIF) that is maintained in accordance to strict data quality protocols.</p>
<p>Retail clients/ participants</p>	<p>LEI are issued on the basis of cost recovery fees, so they will entail one-off costs of approximately 60 euros on the entities who do not already have one and need to obtain it.</p> <p>The requirements leave the door open to potentially cheaper alternatives, provided that they meet the same criteria as the LEI and are deemed "equivalent".</p>	<p>The use of one single standard to identify crypto assets and the entities engaging in these markets allows for better transparency and comparability of information to the benefit of retail investors and entities participating in crypto assets markets.</p> <p>Many entities already obtained an LEI as this code is already required in Europe for entities engaging in financial instruments. These include retail issuers, buyers, and seller that are not financial entities in the strict sense.</p> <p>Access to the full set of LEI and DTI reference data is free of charge for the users, including retail investors and market participants.</p>

## 8.1.5 RTS on the content and format of order book records

### *Problem identification*

126. MiCA introduces new obligations for CASPs operating trading platforms. These CASPs will be obligated to record and store information related to the order-book, and upon request send it to NCAs. Given the novelty of the crypto-asset markets, it's crucial for these CASPs to understand which specific order-book information that needs to be recorded. It is also crucial for these CASPs to understand the exact format in which the order-book data should be maintained and submitted to NCAs. Without a common format, there could be a variety of different formats, which could impose an unnecessary burden on both CASPs and NCAs.
127. Further, NCAs are tasked with duties pertaining to investor protection, market monitoring, and market abuse surveillance of the crypto-asset market. To effectively detect potential market abuse or illegal activities, it is crucial that they receive accurate and comprehensive information on the orders.
128. In order to streamline the reporting process for both CASPs and enable data driven monitoring of NCAs, it is necessary for CASPs to report the data in a standardised format and consistent manner. Additionally, all the parties involved in the crypto-asset transactions and the crypto asset being traded need to be uniquely and consistently identified in a fully automated manner. This is especially relevant for crypto markets where supervisors need to adapt their supervisory efforts and tools with the pace of technological and financial innovation.

### *Policy objectives*

129. The purpose of Article 76(15) and (16) is to define the content and the common format of the order-book records that CASPs that are operating a trading platform are required to maintain. A common format is essential in order for the national competent authorities to fulfil their market monitoring duties.

### *Baseline scenario*

130. In the baseline scenario, the crypto-assets service providers would be subject to the obligation to record the order-book information without specification as to which are the relevant details to be recorded as well as the appropriate format in which order-book information should be maintained and provided to regulators. The result of this would be disparity in the levels of rigour of compliance across trading venue and lack of comparability of order-book information across platforms.

### *Options considered and preferred options*

131. The next paragraphs present the cost-benefit analysis of the main policy options regarding the precise, unique, and consistent identification of the parties to the financial

transaction as well as the crypto asset being traded and the common format in which the relevant information pertaining to orders and transactions should be represented. These elements are the pre-condition for supervisors to be able to monitor the orderly functioning of the crypto assets markets and thus build investors' trust. The various options for formats, and their respective advantages and disadvantages are assessed below, where ESMA has also identified the preferred option resulting from this analysis.

#### Policy issue 1: Defining a common format of the order book records

132. ESMA proposed data format are similar to the format defined in Article 25 of MiFIR/ RTS 24<sup>37</sup>. In the context of MiFIR several formats' options were considered, which is why ESMA conducted a study with external consultants to assess which technical format was the most appropriate for the transaction and reference data reporting. In the study, the following technical formats ISO 20022, FIXML, FpML and TREAM were compared, and the assessment was based on four main criteria (usability of technical formats, implementation feasibility, governance and change control, reusability). The study concluded that ISO 20022 was concluded as the preferred technical format for MiFIR reporting since it provides the highest benefits to regulators without giving rise to undue cost to the industry<sup>38,39</sup>. Based on the study and the feedback received in the Consultation Paper, it was decided that transactions and reference data should be reported in a common XML format and in accordance with ISO 2022 methodology. These options were recently assessed again to account for technology developments and the new upcoming MiCA and MiFIR requirements. For that purpose ESMA commissioned a study<sup>40</sup> on the reporting formats and protocols that could support supervisory reporting requirements more generally. Within the context of the study, ESMA considered the implications of the implementation of its conclusions among other things for the recordkeeping and data transmission obligations under MiCA.
133. The conclusions of the report, as it relates to MiCA recordkeeping and data transmission fit more broadly with ESMA's original proposal in its Consultation Paper of envisaging the use of ISO 20022 standard. Within that choice however, it allows ESMA to propose JSON as the most suitable format for the purpose of these RTS.
134. Similar to the RTS for recording keeping, on-chain data elements have been included as well in order for national competent authorities to be able to monitor on-chain trading activity.

#### *Costs for CASPs*

---

<sup>37</sup> Delegated Regulation (EU) 2017/580 of 24 June 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the maintenance of relevant data relating to orders in financial instruments

<sup>38</sup> [2015-esma-1464 - final report - draft rts and its on mifid ii and mifir.pdf \(europa.eu\)](#)

<sup>39</sup> [2015-esma-1464 annex ii - cba - draft rts and its on mifid ii and mifir.pdf \(europa.eu\)](#)

<sup>40</sup> [ESMA12-437499640-2360 Study on data formats and transmission protocols](#)



135. The cost primarily stems from the higher reporting burden mandated by the level 1 legislation framework. However, ESMA has adopted an approach with the aim of reducing the burden on CASPs while fulfilling its mandate and enabling national competent authorities to access data to do their duties.
136. The costs incurred by CASPs, operating a trading platform for crypto-assets, may be associated with the necessity to either create a new IT system or modify their existing infrastructure. This might be required since they need to ensure that they can collect and store the data related to the order records. Furthermore, CASPs may face additional cost related to the transmission of data to national competent authorities, especially since it must be provided in the JSON format. If the data is not stored in the same format prescribed in the draft RTS, CASPs would need to convert the data. However, this costs arises with any format requirement for provision of data to a national supervisor and, given that JSON is proposed as common format to be used when responding to the requests from any of the national supervisors, the proposed approach minimises costs are there will be a need to adapt to only one conversion.

#### *Costs for supervisors and supervised entities*

137. The primary cost is associated with the initial IT cost, particular because it is not currently used for supervisory reporting by ESMA or commonly used among national competent authorities in the EU. However, the compliance with ISO 20022 is supposed to facilitate the implementation of the JSON messages by market participants. Moreover, the process of developing ISO 2022 messages using JSON syntax would remain quite similar compared to the case of XML. Considering that MiCA introduces new data reporting flows, that do not have an existing data process, the cost of implementing JSON instead of XML or other formats, would be minimal since NCAs will not need to change their current IT system for the sake of using JSON. The costs related to the format and storage of data stems from Level 1 under Article 76(15).

#### *Benefits*

138. The main benefit of JSON is that it is a supported ISO 20022 syntax which would allow the MiCA requirements to stay in line with the requirements under MiFIR, as well as to take into consideration the feedback received during the consultation.
139. Furthermore, given the fact that information in these RTS can be requested at any point by national competent authorities, JSON can be implemented from day-one without the need for a transition period with other formats.
140. Using JSON over XML offer several advantages. Firstly, JSON is more efficient due to it is less verbose nature, which implies higher transmission and processing speed and, thereby, reducing the processing cost. Secondly, JSON is user-friendly due to its higher support by programming tools and the wide availability of skilled resources. Finally, JSON is natively supported by numerous analytical tools, making data ingestion into analytical platforms easier.

141. Lastly, the replies in the Consultation Paper expressed broad support for the format that ESMA proposed for the order records. It permits ESMA to fulfil its mandate without adding an unnecessary burden to the CASPs. Keeping the RTS similar to prior legislative regimes has benefits since it enables for the identification of common trends seen in regular financial markets. For example, fill-or-kill strategies, which according to the respondents are highly frequent when trading in crypto assets. By adopting a reporting standard similar to RTS 24 simplifies the regulatory process for national competent authorities by ensuring a uniform format. This standardization facilitates efficient cross-border surveillance and reduces the complexity of monitoring duties, as it aligns closely with existing frameworks and minimizes the need for additional adjustments.

*Table: Costs and benefits*

Stakeholder groups affected	Costs	Benefits
CASPs	Costs associated with creating a new IT system or modifying their existing infrastructure to ensure that they can collect and store the data related to the order records.	CASPs do not need to convert the information into multiple formats when requested by different national competent authorities. Recordkeeping means that the requirement for the format is only needed when access to information is requested by competent authorities. Burden on CASPs is reduced by leveraging on already established international standards.
Competent authorities	Costs associated with upgrading internal technical systems to accommodate for JSON	JSON is a supported ISO 20022 syntax, which will allow the MiCA recordkeeping requirements to stay in line with the reporting requirements under MiFIR. Adopting a standard similar to RTS 24, widely adopted across the industry, simplifies the regulatory process for national competent authorities by ensuring a uniform format and allows for better data interoperability.
Retail clients	N/A	N/A

### 8.1.6 ITS on standard forms and templates for the crypto-asset white paper

#### *Problem identification*

142. Public disclosure of white paper is important to ensure protection of retail investors. It promotes transparency and comparability of white papers, which enables investors to make informed decisions and to better assess the risk associated with the crypto-asset.
143. For the disclosure of white papers to be beneficial for investors, and to be processed efficiently by competent, a standardised format is essential. A common format ensures consistency across different white papers, making it easier for investors, NCAs, and other stakeholders to compare and analyse different crypto-assets. This also promotes interoperability, as the use of a standardised format allows various systems and software to exchange information seamlessly.
144. Further, MiCA requires the white papers to be drawn up in machine-readable format, which will allow for the data to be processed in an efficient way, however considering the aim is to protect investors it should be in a format that ensures accessibility for everyone regardless of their technical expertise.
145. The main challenge lies in finding a format that benefits stakeholders and national competent authorities, while remaining accessible for investors. Additionally, considering the novelty of the market and the new way of handling white papers, it is important to minimise any unnecessary burden in the process. *Policy objectives*
146. MiCA defines the information that issuers and CASPs must provide within the white papers under Annexes I to III of MiCA. MiCA also requires white papers to be made available in a machine-readable format for all three crypto assets classes.
147. Pursuant to Articles 6(10), 19(9) and 51(9) of MiCA regulation, ESMA is required to define a template for the white papers and a format enabling machine readability of white papers. The objective of this ITS is to provide the templates for the disclosure of the white papers and to specify the machine-readable format for the preparation of the white papers.
148. Since ESMA did not deviate from MiCA Annexes I to III with regards to the templates for the white papers, but only provided a structured form to facilitate CASPs and issuers compliance with their obligations, the costs and benefits specific to the data elements to be provided in the template as part of the L1 obligation have not been assessed. With regards to the costs and benefits linked to the use of specific identifiers, please refer to the section on the RTS on data necessary for classification of white papers.

#### *Baseline scenario*

149. In the baseline scenario without the ITS specifications, persons drawing up white papers would be required to make publicly available white papers in a machine-readable format, without ESMA specifying one single format as mandatory.
150. In such a scenario, persons drawing up a white paper would need to choose which machine-readable format to apply without ESMA specifying one single format for all.

151. In the baseline scenario without the ITS specification, persons drawing up white papers would be required to make publicly available all the fields required in the RTS on data necessary for the classification necessary for the classification of white papers without a common structure and common formats. Furthermore, without the ITS specification regarding the DTI and the LEI, the persons drawing up white papers would be required to make publicly available all the fields otherwise retrievable through the GLEIF and DTIF Registries and be responsible for their data quality (for further details, see the section on the Cost Benefit Analysis for the Draft RTS on data necessary for the classification of white papers).

#### *Policy options and preferred options*

152. The next paragraphs present the cost-benefit analysis of the main policy options regarding the machine-readable format of the MiCA white paper. The various options for the format, and their respective advantages and disadvantages are assessed below, where ESMA has also identified the preferred option resulting from this analysis.

#### **Policy issue 1: Identifying a relevant machine-readable format for the MiCA white paper**

153. The relevant definition of machine-readability is included in the Open Data Directive (EU 2019/1024) to which the ESAP Regulation (2023/2859) makes explicit reference to. This is relevant since all the white papers mandated by MiCA will need to be available in ESAP starting from the year 2030, therefore it is important that the definitions applied in the MiCA context are consistent with those applied in the ESAP context.
154. Considering that the aim of the MiCA regulation is to ensure protection of retail investors, ESMA proposed in its Consultation Paper to specify iXBRL as the format of the white papers since it allows for both machine-readability (which is mandated by the MICAR) and human-readability (which is deemed highly desirable given the retail investor-focus of the MiCA white papers).
155. As indicated in the Consultation paper, ESMA commissioned an external contractor to conduct a study to understand which alternative formats exist which could be relevant for the purpose of the MiCA white papers and to obtain recommendations regarding the most suitable one. The study commissioned by ESMA considered several formats options, namely CSV, JSON, PDF, XBRL, XLS and inline XBRL. They were assessed against a set of criteria, namely fitness for purpose (machine-readability and human readability) and fitness for future (level of adoption, reusability, governance, non-proprietary, implementation feasibility).
156. On the basis of the study, the external contractor recommended iXBRL. As no other format was deemed to fulfil all the criteria chosen for this assessment, no other option was assessed in detail. Please refer to ESMA's website for the [detailed analysis conducted](#).

157. The next paragraphs present the cost-benefit analysis of the iXBRL as the machine-readable format for the MiCA white paper.

#### *Costs*

158. The study commissioned by ESMA concluded that the incremental costs of imposing iXBRL compared to other machine-readable formats (such as XML or JSON) is not significant. For issuers, iXBRL will result in expenses associated with converting documents into iXBRL format, which might require the services of external providers for iXBRL tagging (which are likely to charge between EUR 200 and 1350 per white paper) or the use of a conversion tool made available by ESMA. The latter option would not entail additional costs for entities. In light of the positive feedback received during the consultation, ESMA is intending to provide a simple converter to iXBRL format for the MiCA white paper, further developing the PoC proposed during the Consultation.

159. NCAs may also face costs due to the necessity of upgrading their technical systems to accommodate iXBRL. However, national competent authorities are already developing their technical capabilities to handle iXBRL due to the ESEF reporting format.

160. It should also be acknowledged that ESEF requires far more complex filing and validation rules compared to the MiCA regulation, and together with the growing adoption of iXBRL in the industry it is suggested and confirmed by the independent study commissioned by ESMA that the incremental costs of processing MiCA white papers in iXBRL format will be minimal.

#### *Benefits*

161. iXBRL is both machine and human readable, which is a useful feature that enhances transparency and accessibility for all users, especially retail users.

162. Specifying one format, rather than leaving the choice to issuers/CASPs, ensures consistency and allows for a standardised way of processing white papers for users. It also prevents the risk that issuers/CASP will adopt PDF, which does not fulfil the requirements of machine-readability and would therefore lead to a breach of the Level 1 requirements.

163. iXBRL is already a standard reporting format in many jurisdictions around the world, as confirmed by the independent study commissioned by ESMA, and it is consistent with other EU Data initiatives such as ESEF and SFDR and could potentially be reused for other similar textual based disclosures covered by ESAP.

#### *Conclusions*

164. ESMA's proposal to use iXBRL is based on an independent study and on the outcome of the Consultation. ESMA is aware of the potential cost for the industry, however considering the growing adoption of iXBRL and the fact that ESMA will make available a

tool for the conversion of the white paper into iXBRL format, the costs will most likely be minimal.

*Table: Costs and benefits*

Stakeholder groups affected	Costs	Benefits
Persons drawing up white papers and CASPs	For issuers, iXBRL will result in costs associated with converting documents into iXBRL format, which might require the services of external providers for iXBRL tagging (which could cost between EUR 200 and 1350 per white paper)	Consistency in disclosures and standardised methods to process white papers for end-users
Competent authorities	Costs associated with upgrading internal technical systems to accommodate iXBRL	iXBRL is consistent with other EU data initiatives such as ESEF and SFDR and could potentially be reused for other similar textual based disclosures covered by ESAP
Retail clients	N/A	Human and machine readability of white papers ensures adequate transparency, including for retail clients holding these crypto-assets

### 8.1.7 RTS on the data necessary for the classification of white papers

165. ESMA is mandated to establish a register of crypto-asset white papers, of issuers of asset-referenced tokens and e-money tokens, and of crypto-asset service providers. Pursuant to Article 109(8), ESMA needs to specify in the RTS the data necessary for classification, by type of crypto-asset, of crypto-asset white papers, including the legal entity identifiers in the register.

#### *Problem identification*

166. To protect investors, it is important that they are well informed about the characteristics, functions, and risk of the crypto-asset that they have invested or intend to invest in. The information pertaining to the crypto-assets must also be accessible for investors in an easy way. MiCA proposes the creation of a register where investors can search for white papers using a standardised set of search criteria.

167. Furthermore, it is necessary to identify the persons drawing up the white papers, the crypto-asset, and the related white paper. For the identification process to be efficient for both investors and national competent authorities, it is essential to use appropriate identifiers. These identifiers should take into account the global scope and innovative nature of the crypto-asset market.

#### *Policy objectives*

168. The scope of the register is mainly connected to ESMA IT system, and its impact will be on national competent authorities. However, the need for certain data for the ESMA register implies that, in order for national competent authorities to be able to provide to ESMA such data, that data needs to be provided by the reporting entities to the national competent authorities in the first place. Therefore, the costs and benefits of the data needed for the purpose of the ESMA registers are assessed in the CBA related to this RTS, even if the obligation (and therefore cost/effort) to provide such data will lie with CASP/issuers entities on the basis of the white paper templates mandated under the ITS on standard forms and templates for the crypto-asset white paper.
169. It was deemed that the most relevant data the costs and benefits of which should be assessed are the identifiers, namely the LEI and the DTI.

#### *Baseline scenario*

170. In the baseline scenario without the RTS specifications, persons drawing up white papers and national supervisors would be responsible for the maintenance and data quality of all the fields retrievable through the DTIF and the GLEIF registries.

#### *Policy options and preferred options*

171. The next paragraphs present the cost-benefit analysis of the main policy options regarding the identifiers to be used for parties, crypto assets, and white papers pertaining to those crypto assets. The various policy options, and their respective advantages and disadvantages are assessed below, where ESMA has also identified the preferred options resulting from this analysis.

#### **Policy issue 1: Identifying Legal Entities**

172. It is crucial for investors' protection that the persons responsible for drafting the white papers are identified with a unique and widely used identifier, particularly to ensure that the information published in ESMA register pertains to the entities described in the white papers and to ensure that the information disclosed pursuant to MiCA can be connected to other disclosures made available by issuers/CASPs pursuant to other legislations. In order to identify the persons drawing up the white paper, ESMA proposes to use the Legal Entity Identifier (LEI).



173. No alternative to the LEI was identified in the consultation by any of the respondents. It has also been noted by the respondents to the Consultation as well as the national supervisors that the alternative of using national identifiers would not be beneficial, as there are currently no relevant identifiers related to issuers or CASPs which could be useful for the purpose of a register of white papers.

#### *Costs for issuers/offerors and CASPs*

174. LEI is a paid-for identifier, therefore requiring an LEI would impose some limited costs to the entities that do not already have one (the average LEI registration fee in the EU amounts to 60 euros per year). The broad support in the Consultation Paper indicates that this is not perceived as a significant cost.
175. On balance, the inclusion of the LEI in the white papers will allow for a reduction in the burden imposed on issuers and CASPs since the GLEIF database stores several data elements characterising the legal entity which are maintained in a standardised manner, following strict data quality protocols. When the LEI is reported, NCAs will be able to source these additional information directly from the GLEIF database rather than asking for them to be reported in each white paper. This will minimise the burden for issuers/offerors and it will reduce the risk of these fields being filled out incorrectly. Having to collect and periodically check the additional information characterising the legal entity separately from the LEI will entail higher costs on the persons drawing up the white paper.

#### *Costs for investors, market participants and regulators*

176. While LEI may entail some costs for the issuers, consolidated access to the full set of LEI reference data is free of charge for the users, retail investors, market participants and regulators. Today, the financial institutions that service parties to financial instruments transactions use the LEI as a source for the basic customer information meaning free and automated access to the basic customer information data for their own internal operations.

#### *Benefits*

177. The LEI is a code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). The publicly available LEI data pool maintained by the Global Entity Identifier Foundation (GLEIF) is the only global directory which provides for free information about the identification of legal entities participating in financial transaction. Therefore, it is a unique key to standardized information on legal entities globally and, as indicated in the [Digital Finance Strategy for the EU](#), it consistently facilitates the use of RegTech tools for reporting and SupTech tools for data analysis by authorities in a digital environment.
178. The LEI has already been tested and used by the ESAs as the identifier that enables proper validation of the entity submitting the reports as well as the entities identified in

the reports to be published in the central registries of financial information at EU level. The availability of the central GLEIF database containing standardised reference data linked to legal entities, following strict data quality protocols and allowing daily downloads of its full content is key for these purposes. Without such system, it becomes challenging for the ESA to validate that the data concerning the legal entities actually pertains to the entity concerned.

179. In addition, the LEI is used to disseminate information from the centralised databases to the different national competent authorities at member state level. This is because the LEI facilitates linking different databases and other sources of information available at the national and international level, especially since it is already mandated in many existing pieces of EU and national legislation for reporting purposes. It would therefore be very beneficial to data users, including NCAs, to be able to link the information disclosed pursuant to MiCA to other disclosures by the same entities pursuant to other legal obligations.
180. As of now, the ESAs have not identified any local or regional identifier that could be considered fit for these purposes and thus would constitute a valid “alternative” legal entity identifier compared to the LEI. Furthermore, LEI is a global international standard, it is therefore the most appropriate choice for crypto asset markets, which are global by nature. However, the text in the technical standards leaves the door open to alternative identifiers should any of those be deemed as fulfilling the same criteria as the LEI in the future.

#### Policy issue 2: Identification of crypto assets and white paper pertaining to those crypto assets

181. ESMA proposes to use the Digital Token Identifiers (DTI) for the purpose of identifying crypto-assets and the Functionally Fungible Group Digital Token Identifier (FFG DTI) to identify white papers pertaining to those crypto assets.

##### *Costs for persons drawing up the white paper*

182. Using DTI as the unique identifier would cause some limited additional costs for persons drawing up a white paper. As of today, registering a crypto asset in the DTI registry is free of charge but future one-off registration fees are being considered and consulted. The DTI Foundation which maintains the DTI registry and assigning of DTIs is, at the time of publication of this Final Report, running a consultation on its fee structure.
183. In addition, ESMA estimates that having to collect and periodically check the additional information characterising the legal entity separately will entail higher costs on the persons drawing up the white paper.

##### *Costs for users and supervisors*

184. The proposal in the DTIF fee consultation provides for free access to the DTI registry via the DTIF website and in a machine-readable format for all users. Therefore, retail

investor will have free and immediate access to the information in a standard format that allows machine readability. DTIF also confirms that regulators and supervisors will not be subject to fees (similar to the DSB model for ISIN and UPI).

185. The more sophisticated users with a need to access to the full DTI database on an ongoing basis with machines, would be charged a cost-recovery fee to have a live API-based access to the DTI registry. Ancillary services going beyond a cost-recovery fee would include the ability to reserve DTIs and premium web search lookups, but these services will not be needed for the purpose of compliance with the requirements envisaged in ESMA technical standards.
186. As the maintenance agency of an ISO standard, the DTIF must abide by cost-recovery services that are fair, reasonable, and non-discriminatory lest they lose their ISO contract. Cost Recovery means that fees or other revenues associated with Services rendered generate only sufficient funds to cover the costs attributable to those Services. It may include an allocation of overhead expenses incurred directly by the DTIF that can be shown to be required to meet the Services rendered. Such overhead costs must be reasonable. Other costs not directly related to such Services, or costs related to other services, shall not be included. As such, it is expected that there will be no increase in the fees and that there will be a substantial decrease in fees linked to base services (i.e., token registration) once cost-recovery fees have surpassed the cost of the service build. In its consultation on the cost-recovery model<sup>41</sup>, the DTIF has highlighted that:

As part of annual review and consultation, any excess revenue over costs will be used to reduce fees in subsequent years. Factors beyond user base and volume requests are also expected to reduce future fees for DTI Allocation, such as:

Further automation of submission and verification procedures  
Greater capacity to handle bulk DTI Allocations (and subsequent discount rate based on lower marginal cost of DTI allocation).

Any excess revenue over costs will be used to reduce subsequent user-fees as part of a regular fee revision process. Any fee variation requires adherence to the DTI Foundation's governance framework, which includes a public consultation to validate proposed changes.

187. The DTI is, so far, the only standard as defined at the Union level which is a) unique; b) neutral; c) reliable; d) open source; e) scalable; f) accessible; g) available at a reasonable cost; and h) subject to an appropriate governance framework. For example, the only alternative mentioned (by one respondent) in response to ESMA's consultation, the FIGI, does not meet the criteria of a) uniqueness, g) availability at a reasonable cost, and h) appropriate governance. Indeed, the FIGI does not allow users to identify crypto assets below the asset level (i.e., on different DLTs) free of charge. This means that in order to

---

<sup>41</sup>DTIF Consultation on cost-recovery model: <https://dtif.org/wp-content/uploads/2024/06/DTI-consultation-on-cost-recovery-model-June-2024.pdf>

meet the MiCA granularity requirements in the respective technical standard, charges will apply and, given that FIGI is a proprietary identifier as it owned and governed by a private company, such charges will not be applied on a cost recovery basis.

188. In addition, the adoption of the DTI will also allow for a reduction in the burden imposed on issuers and CASPs since the DTIF database stores several data elements characterising the crypto asset which are maintained in a standardised manner, following strict data quality protocols. When the DTI is reported, NCAs will be able to source these additional information directly from the DTIF Registry rather than asking for them to be reported in each white paper. This will minimise the burden for issuers/offerors and it will reduce the risk of these fields being filled out incorrectly or becoming out of date.

### *Benefits*

189. The main benefit of DTI for the purpose of the register of white papers is that it is defined by the International Organisation for Standardisation's ISO 24165 and offers linkage across the asset level to another ISO standard with the ISIN<sup>42</sup> and plans are ongoing to include a link with the LEI of the issuer in the DTIF registry, Token level, and DLT level. Using an international standard identifier such as DTI allows investors to properly compare different crypto-asset white papers and national competent authorities to perform their assessment on the basis of harmonised information.
190. Concerning the general benefits of DTI, please refer to the respective section in the record keeping Section 8.1.4 above. That section includes an overview of the cost and benefits related to LEI and DTI.

## **8.1.8 ITS on the technical means for appropriate public disclosure of inside information**

### *Impact of the draft ITS under Article 88(4) of MiCA*

191. As per Article 15(1) of Regulation (EU) No 1095/2010, any draft implementing technical standards developed by ESMA shall be accompanied by an analysis of 'the potential related costs and benefits' of the technical standards.
192. Article 88(1) MiCA requires issuers, offerors or persons seeking admission to trading of crypto assets, to inform the public as soon as possible of inside information that directly concerns them, in a manner that enables fast access as well as a complete, accurate and timely assessment of the information by the public. The same entities are required to post and maintain on their website, for a period of at least five years, all inside information that they should publicly disclose.

---

<sup>42</sup> [ISIN-DTI Complementary Standards Bridging Traditional and Digital Markets < DTIF](#)

193. In addition, Article 88(2) of MiCA permits the delay of the disclosure of inside information where (i) immediate disclosure would be likely to prejudice a legitimate interest of the relevant party; (ii) the delay of the disclosure is not likely to mislead the public, and (iii) the confidentiality of the information is ensured.
194. The next paragraphs present the cost-benefit analysis of the main policy options included in this final report on the technical means for (a) appropriate public disclosure and (b) delaying the public disclosure of inside information, pursuant to Article 88 of MiCA.

#### *Problem identification*

195. Public disclosure of inside information is essential to reduce the risk of insider dealing and ensure that investors timely receive price sensitive information. For such disclosures to be effective, inside information should be disseminated to as wide as public as possible and in a non-discriminatory manner. Thus, issuers, offerors or persons seeking admission to trading should use means for dissemination that ensure investors are promptly informed in a non-discriminate manner.
196. Further, the lack of a standardised technical means for delaying public disclosures may lead to diverging practices across Member States, impeding uniform application of the provision regarding delays of disclosure found in Level 1 of MiCA.
197. Against this background, MiCA mandates ESMA to develop ITS to determine the technical means for (a) appropriate public disclosure and (b) delaying the public disclosure of inside information under Article 88 of MiCA.

#### *Policy objectives*

198. The strategic objective of the draft ITS is to (i) identify the appropriate means for disclosure of inside information which ensures investors are promptly informed in a non-discriminatory way; and (ii) harmonise the technical means issuers, offerors or persons seeking admission to trading should use to delay the disclosure.

#### *Baseline scenario*

199. The baseline scenario is the situation where issuers, offerors or persons seeking admission to trading must comply with the obligation under Article 88 of MiCA, without any further specification of the means for ensuring proper public disclosures of inside information or for the technical means to delay such disclosures.
200. As these obligations have a rather general nature, this may have a significant impact. Firstly, the absence of requirements for the media to be used for such disclosures may lead some issuers or offerors to rely on media with limited reach or to barriers to access that may render the disclosure discriminatory. This would directly result in information asymmetry, with the consequence of potential harm to confidence in and efficiency of markets in crypto-assets.

201. Furthermore, publication of the information on the website may be done in a way that does not allow users to easily access or verify the information, creating doubts about the reliability of the information disclosed. This may also harm confidence and efficiency of markets in crypto-assets.
202. Similarly, the lack of any requirements in respect to the technical means of delaying the disclosure may lead to non-standardised approaches that would undermine adherence to the principles of integrity, confidentiality, or rapidity of the transmission of the relevant notification to the NCA. In addition, the use of different technical means to delay public disclosures presents an obstacle to the uniform application of the same obligation across Member States.

#### *Options considered and preferred options*

203. This section presents the main policy options discussed and the decisions made when developing the draft ITS. The various policy options, and their respective advantages and disadvantages are assessed below, where ESMA has also identified the preferred options resulting from this analysis.

#### **Policy issue 1: Means for public disclosure of inside information**

204. ESMA considered two policy options:

**Option 1a:** Set out only high-level requirements for the technical means for public disclosure of inside information;

**Option 1b:** Add to general requirements, an indication of the media which are used by crypto investors to collect information on crypto assets to make informed decisions.

205. Option 1a was regarded as not properly reaching the objective of the mandate, as it would have failed to identify the most adequate means to ensure investors in crypto assets are informed. ESMA believes that option 1a did not take into consideration the specific features of the crypto environment, notably, the different media used by investors in crypto assets in comparison to investors in traditional financial instruments to collect information. As a result, this option would run the risk of permitting disclosures via means not relied upon by the relevant public.
206. Under option 1b, issuers, offerors or persons seeking admission to trading, when assessing the means to be used for the disclosure, are required to consider the specific media used by crypto investors to collect information on crypto-assets (e.g. social media and web-based platforms). This should ensure the use of adequate means to reach crypto investors, and therefore effective dissemination.
207. In addition, ESMA notes that the media included in the draft ITS would generally meet the objective of reaching a wide, cross-border public without incurring in high fees for those making the disclosures.

208. Thus, Option 1b was chosen as the preferred option.

#### Policy issue 2: Means for the delay of public disclosure of inside information

209. ESMA considered two policy options:

**Option 2a:** Replicate the technical means indicated under MAR ITS for delaying the disclosure of inside information;

**Option 2b:** Specify new technical means to delay the disclosure of inside information related to crypto assets.

210. Option 2a considers that MiCA and MAR have comparable requirements regarding the delayed disclosure of inside information. Furthermore, ESMA sees merit in aligning the regime for disclosure of inside information under MAR and MiCA to leverage on the experience developed under MAR and streamline the regulatory framework on inside information disclosure.

211. Option 2b would have requested a different approach for delay the disclosure of inside information under MiCA, in respect to the means already used under MAR. No aspect of the crypto asset market would have justified the use of a different approach. In addition, it was considered, a new approach may have created interpretative doubts.

212. For the above reasons, Option 2a was chosen as the preferred option.

#### *Cost-benefit analysis*

213. The draft ITS for appropriate public disclosure and for delaying the public disclosure of inside information are expected to result in both costs and benefits to applicants and NCAs.

#### *Costs*

214. It should be preliminarily observed that since the requirements on the disclosure of inside information are provided under MiCA, the impact of the draft ITS should be considered having in mind those legal provisions.

215. In particular, the costs related to the design of a process to identify, publish and disseminate the inside information, or those related to the creation of a website when persons subject to the obligation do not already have one, arise directly from the disclosure obligation enshrined in Article 88(1) of MiCA. Similarly, the cost in relation to the design of a process for the delay of the inside information originates from Article 88(2) and Article 88(3) of MiCA.

216. In this context, the on-going cost of disclosing inside information would largely depend on the number of disclosures and is represented by the resources dedicated to the disclosure.



217. Against this background, the ITS adds one-off costs consisting in adapting an existing website to the requirements of the draft ITS, e.g. by ensuring that disclosure of inside information is located in an easily identifiable section of the website, organised in chronological order.
218. In addition, the media identified in the ITS as adequate for the disclosure may also request a fee for the publication (e.g. newswires syndicated in traditional media outlets), even though in most cases posting on such media is free of charge (e.g. social media, web-based platforms). In respect to the delayed disclosures, the main expected one-off and on-going costs for persons subject to the disclosure obligations arising from the ITS are likely to relate to the design, implementation and maintenance of the technical means to be used for the process of delaying the disclosure of inside information (e.g. the maintenance in a durable medium of a set of information related to the process of delaying the disclosure).
219. Other cost drivers to consider could include the nature of the means for transmitting notifications to NCAs: the ITS requires issuers to use the electronic means published by the competent authority on its website, and this could imply the development of adequate IT infrastructure if the one already in place is not compatible with the electronic means selected by the NCAs. Such electronic means must ensure that completeness, integrity and confidentiality of the information is maintained during the transmission and therefore is possible that not all issuers are already equipped with this type of IT means. However, it is worth noting that compliance with such requirements is not expected to generate significant costs.
220. For **NCAs**, the ongoing cost is connected with the monitoring of the disclosure obligation, which according to the ITS may include the new typologies of media.
221. In respect to delayed disclosure, the ITS reduces the cost to the minimum for NCAs by leveraging on the systems and procedures already in places to receive similar notification under MAR.

### *Benefits*

222. In terms of benefits, the draft ITS will promote convergence and foster clarity and predictability in respect to disclosure of inside information. The harmonised application requirements also promote a level playing field among issuers, offerors or persons seeking admission to trading of crypto assets, no matter their home Member State.
223. In addition, the draft ITS promotes the integrity and the efficiency of markets in crypto assets, ultimately increasing the confidence of the investors in this market.

*Table: Costs and benefits of the draft ITS on disclosure of inside information*

Stakeholder groups affected	Costs	Benefits
<b>Issuers, offerors or persons seeking admission to trading of crypto assets</b>	<p>Initial costs to amend the website to comply with the requirements of the draft ITS</p> <p>Ongoing costs for the resources dedicated to the disclosure.</p> <p>Fees where media charge for the posting or the publication.</p> <p>Costs of implementation and maintenance of the IT infrastructure to used for the process of delaying the disclosure of inside information in compliance with the ITS.</p>	<p>Clarity and predictability in respect to the disclosure obligation.</p> <p>Level-playing field.</p> <p>Increased confidence of investors in crypto asset market.</p>
<b>Competent authorities (NCAs)</b>	<p>Initial one-off costs to amend or implement internal process for monitoring compliance with the disclosure obligation in respect to crypto assets.</p>	<p>Harmonisation and level-playing field.</p> <p>Clarity on means to be used for the disclosure and the relevant delay.</p> <p>Increased confidence of investors in crypto asset market.</p>

## 8.2 Annex II: Advice of the Securities and Markets Stakeholder Group

### **SMSG advice to ESMA on its Consultation Paper on Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – second consultation paper**

#### **8.2.1 Executive Summary**

The SMSG provides opinions and comments on a selection of issues discussed in the second MiCA consultation paper.

Proportionality. Proportionality is key to avoiding barriers to small-size players, holding constant all measures targeted to the soundness of the crypto ecosystem. The SMSG supports the approach to proportionality for business continuity proposed in the draft RTS, including the proposed self-assessment, as it allows each entity to calibrate business continuity measures on their own needs. The SMSG also recommends that proportionality, where appropriate, should be taken into account in other aspects of MiCA, where these do not compromise overarching safety and soundness considerations. This recommendation rests on the idea that a ‘one size fits all’ approach may limit the participation of small-size players and ultimately also the competitiveness of the EU crypto ecosystem with respect to other jurisdictions.

Governance. The draft RTS on organisational arrangements establishes that the CASP’s management body must endorse and regularly review the business continuity policy. The SMSG supports the approach proposed in the draft RTS, including the roles of the CASP’s management body to define, endorse, implement and review the business continuity policy. The SMSG does not see a need to require the establishment of a business continuity function to oversee the obligations in the RTS, leaving this possibility to the decision of the CASP’s management body, also taking into account considerations related to proportionality. The SMSG also highlights that CASPs’ governance is key to build a robust crypto ecosystem.

Measures for permissionless DLT. The consultation paper clarifies that CASPs that intend to conduct their services on permissionless DLTs should make their clients aware of the risks that this entails at the point when their clients first access those services. ESMA encourages CASPs to explain to their clients that their liability does not extend to permissionless DLTs. The SMSG supports the proposal to require CASPs to communicate externally with their clients in the event of a service disruption involving a permissionless DLT. The SMSG recommends that external communications are performed making sure that users are actually reached and aware of the issues, also with the establishment of temporary contact points. The SMSG also recommends that appropriate disclosure should be carried out when users first access those services to make them aware of the risks associated to permissionless DLT and the scope of CASPs’ liability (that includes their own smart contracts and does not extend to permissionless DLT). 2

The specialness of the user base. MiCA requires CASPs to keep records of all crypto-asset services, activities, orders, and transactions undertaken by them. Concerning clients that are not eligible for a LEI, ESMA proposes to use the list of national identifiers, which are dependent on the client's nationality, prescribed by MiFIR. The SMSG supports the proposal to rely on the methods for client identification that are used under MiFIR, having considered that the expected user base of crypto services may be largely represented by natural persons, not acting in a business capacity, who are not eligible for a LEI. The SMSG also highlights that the special composition of the users' base of crypto services deserves careful attention with regard to the communication methods used to reach crypto users.

Pre-trade transparency for AMMs. ESMA proposes to include a description and the related pre-trade transparency requirements for Automated Market Makers (AMMs) particularly in a Decentralised Exchange (DEX) context. The draft RTS requires the disclosure of the mathematical equation used to determine the price and the quantity of the crypto-assets in the liquidity pools. The SMSG supports the proposal to require the publication of the mathematical equation for price and quantity, as this requirement makes market participants aware of the price setting rule. The SMSG suggests to disclose details to enable market participants to understand the difference in the price discovery with respect to more widely known methods to set the price.

White paper. Crypto-asset white papers should contain information, among other things, on the project to be carried out with the capital raised. White papers for 'other cryptos' are expected to include the planned use of collected funds. The SMSG believes that investors also need to know the actual use of the funds after the issuance (not only the expected use at the time of the white paper). Issuers of 'asset-referenced tokens', in addition to the information provided in the white paper, should also provide information on an ongoing basis. The SMSG highlights the need to provide ongoing information to the holders of other cryptos (not only to the holders of 'asset-referenced tokens').

Cooperation. ESMA requested the opinion of the SMSG regarding two RTSs and two ITSs relating to (i) the exchange of information between competent authorities, (ii) procedures, forms and templates for the exchange of information between competent authorities, (iii) procedures, forms and templates for exchange of information between competent authorities and ESMA/EBA, and (iv) the template for cooperation with third-country authorities. The SMSG supports the adoption of the proposed technical standards.

## 8.2.2 Background

1. On 5 October 2023, ESMA released the second MiCA Consultation Paper as part of a series of three packages. Each package includes a number of draft implementing technical standards (RTS) and draft implementing technical standards (ITS). The first consultation 3 paper was published on 20 July 2023 and the SMSG provided an Advice

to ESMA on 6 October 2023. This second Consultation Paper covers the following aspects:

- i. sustainability indicators on adverse impacts on the climate and the environment;
  - ii. continuity and regularity in the performance of crypto services;
  - iii. offering pre- and post- trade data to the public;
  - iv. record keeping obligations for crypto-asset service providers (CASPs);
  - v. machine readability of white papers and white papers register;
  - vi. technical means for appropriate public disclosure of inside information.
2. In parallel, ESMA produced a set of draft technical standards which specify information relating to cooperation between national competent authorities (NCAs), European Supervisory Authorities and third-country authorities. On 10 October 2023, ESMA requested the SMSG to provide advice on such draft technical standards by 14 December 2023.
3. In this Advice, the SMSG replies to specific questions raised in the Consultation Paper and provides comments on more general issues that are related to the specific questions. The SMSG also provides its advice on the draft technical standards on cooperation.

### **8.2.3 Comments on aspects included in the draft RTS and ITS**

#### **Proportionality**

4. MiCA Regulation builds upon available regulatory frameworks on different aspects. For example, to ensure continuity and regularity in their performance, CASPs are required to employ appropriate and proportionate procedures to ensure resilient and secure ICT systems, as required by Regulation (EU) 2022/2554 (DORA)<sup>43</sup>. Along the same lines, ESMA has relied on standard Business Continuity Management (BCM) requirements found in existing regulations as a guide<sup>44</sup>. Specifically, ESMA relies on two RTS under MiFID II (for investment firms, and trading venues) as they elaborate general principles for business continuity arrangements.
5. The SMSG understands that business continuity requirements contribute to the maintenance of orderly markets by limiting, to the extent possible, undue losses for clients of CASPs in the event of a disruptive incident. The SMSG also highlights the need

---

<sup>43</sup> CASPs are already included in the scope of DORA as a type of 'financial entity' listed in Article 2(1)(f) of DORA.

<sup>44</sup> Paragraph 76 of the consultation paper makes clear that the business continuity management requirements in the draft RTS follow the standardised playbook seen in other sectoral regulations (e.g., MiFID II). These include (i) organisational arrangements, (ii) the business continuity policy (including independent auditing), (iii) business continuity plan, and (iv) periodic review and testing of the business continuity policy.

to strike the right balance between the soundness of the crypto ecosystem and the need to avoid barriers to new entrants.

6. Proportionality is explicitly included in this consultation with respect to the continuity dimension. Indeed, like DORA, MiCA calls for a “proportionate approach” whereby certain CASPs under scope should not be subject to “excessive and disproportionate administrative burden” (Recital 27 of MiCA) and the business continuity requirements should “tak[e] into account the scale, the nature and range of crypto-asset services provided” (Article 68(8) of MiCA).
7. The draft RTS on continuity includes – in Article 6 – a general proportionality principle which is meant to specify the language found in Article 68(8) on the “scale, the nature and range of crypto-asset services provided”. Paragraph 2 of Article 6 goes further by building on this proportionality principle with a mandatory ‘self-assessment’ to be completed by the CASP. The self-assessment is a concept once-again borrowed from MiFID and the rationale for including this provision is to ensure that CASPs are taking stock of the risk factors that may interrupt regularity or continuity in the performance of their services which may trigger the business continuity plan (and affect its execution). The criteria of this self-assessment are available in the Annex of the RTS.
8. The SMSG supports the approach to proportionality for business continuity proposed in Article 6 of the draft RTS, including the proposed self-assessment, as it allows each entity to calibrate business continuity measures on their own needs<sup>45</sup>. The SMSG also recommends that proportionality, where appropriate, should be taken into account in other aspects of MiCA, where these do not compromise overarching safety and soundness considerations such as, inter alia, investor protection, antifraud requirements, AML/FT, and any risk-leakage to the broader financial system. Proportionality is key to avoiding barriers to small-size players, holding constant all measures targeted to the soundness of the crypto ecosystem. This recommendation rests on the idea that a ‘one size fits all’ approach may limit the participation of small-size players and ultimately also the competitiveness of the EU crypto ecosystem with respect to other jurisdictions. As highlighted in the SMSG Advice concerning the first consultation paper on MiCA, to protect EU investors, an important challenge is to bring crypto services into the scope of EU regulation. Barriers to small-size players may result in the unintended consequence of increasing the activity not in scope.

## Governance

9. Article 68(4) of MiCA requires CASPs to adopt policies and procedures that are sufficiently effective to ensure compliance with MiCA and Article 68(6) requires the

---

<sup>45</sup> See Section 4.3.3 of the consultation paper (Proportionality principle) and Q19 (In Art. 68(8), CASPs are required to take into account the scale, nature, and range of crypto asset services in their internal risk assessments. Is there support for this general principle on proportionality in Article 6? Do you support the proposed self-assessment under Article 6(2) and in the Annex of the draft RTS?).

management body of CASPs to assess and periodically review the effectiveness of the policy arrangements and procedures.

10. Article 2 of the draft RTS on organisational arrangements establishes that the CASP's management body must endorse and regularly review the business continuity policy. The article further specifies MiCA Level 1 by requiring the management body to review the business continuity policy on at least an annual basis, specifying "periodically" set forth in Article 68(6) of MiCA.
11. The SMSG supports the approach proposed in Article 2 of the draft RTS, including the roles of the CASP's management body to define, endorse, implement and review the business continuity policy. The SMSG does not see a need to require the establishment of a business continuity function to oversee the obligations in the RTS, leaving this possibility to the decision of the CASP's management body, also taking into account considerations related to proportionality<sup>46</sup>.
12. The SMSG also highlights that CASPs' governance is key to build a robust crypto ecosystem. As known, recent cases of malpractice may hinder the reputation of the crypto ecosystem and ultimately its healthy growth. Against this background, a careful assessment of the CASPs' governance is also important for market confidence and systemic risk.

### **Measures for permissionless DLT**

13. ESMA proposes following the structure of business continuity management measures established by the relevant RTS in MiFID II. To clarify the general principal on proportionality in Article 6 (see also previous Section 3.1), the draft RTS on continuity introduces – in Article 1 – a definition of "permissionless distributed ledger technology" (permissionless DLT) adapted from a recent consultative document of the Financial Stability Board (FSB)<sup>47</sup>. The FSB defines "permissioned DLT" when entities – normally selected and authorised beforehand – perform validation and settlement of transactions, and "permissionless DLT" when validator nodes (miners) can be set up by anyone fulfilling the technical requirements and the protocols. The Consultation Paper refers to permissionless DLT as publicly accessible DLT such as Ethereum, that does not gatekeep access to the validator network.
14. ESMA proposes to add several provisions that would acknowledge the differences between permissionless DLTs and permissioned DLTs in the context of business continuity. These provisions acknowledge the novel risks posed by permissionless DLTs without losing sight of the fact that, ultimately, CASPs are responsible for deciding how

---

<sup>46</sup> See Section 4.3.2 of the consultation paper (Business continuity management), Q16 (Should this RTS also specify that CASPs should establish a business continuity management function (to oversee the obligations in the RTS)? In your view, does this fall within the mandate of 'measures' ensuring continuity and regularity?) and Q17 (Are there other organisational measures to be considered for specific CASP services?).

<sup>47</sup> See Annex 1 of Financial Stability Board, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, Consultative document, 11 October 2022, available at <https://fsb.org/wp-content/uploads/P111022-3.pdf>.



best to manage this type of operational risk and reflecting this in their business continuity arrangements for a 'timely recovery and response' to disruptive incidents. As stated in paragraph 71 of the Consultation Paper, the differentiated approach for permissioned and permissionless DLT should not come at the expense of consumer protection, nor is it an invitation for CASPs to engage in 'decentralisation arbitrage'.

15. Article 4(2)(e) of the draft RTS on continuity establishes that the business continuity plan shall provide procedures for timely external communications with clients in the event of a disruption involving a permissionless DLT. Recital 3 of the draft RTS clarifies that such communication should include essential information for the client, including updates on when services may be expected to be resumed, information related to the reason for the disruptive incident affecting a distributed ledger once such information becomes available, how many DLT network nodes have been affected, whether client funds are at risk, and how the distributed ledger will be brought back online (e.g., a roll-back to a previous timestamp). ESMA believes this information should constitute an important feature of a CASP's business continuity planning.
16. The Consultation Paper clarifies that, as part of their duty in Article 66 of MiCA to act in the best interests of clients, CASPs that intend to conduct their services on permissionless DLTs should make their clients aware of the risks that this entails at the point when their clients first access those services. In the same spirit of disclosure, ESMA would also encourage CASPs to explain to their clients that their liability does not extend to permissionless DLT. The Consultation Paper also clarifies that – being conscious of the distinction between an issue related to a CASP smart contract vs. operational issues with the underlying DLT – CASPs should remain liable for any losses related to their own smart contracts, such as hacks or exploits, regardless of whether they are deployed on a permissionless or a permissioned DLT.
17. The SMSG supports the proposal to require CASPs to communicate externally with their clients in the event of a service disruption involving a permissionless DLT<sup>48</sup>, having considered that such a requirement would imply a more orderly return to service once the incident is resolved. The SMSG recommends that external communications are performed making sure that users are actually reached and aware of the issues, also with the establishment of temporary contact points. The SMSG also recommends that appropriate disclosure should be carried out when users first access those services to make them aware of the risks associated to permissionless DLT and the scope of CASPs' liability (that includes their own smart contracts and does not extend to permissionless DLT).

---

<sup>48</sup> See Section 4.3.1 of the consultation paper (Measures for permissionless distributed ledger technology) and Q15 (Do you consider subparagraph (e) in Article 4(2) on external communications with clients in the event of a disruption involving a permissionless DLT appropriate for the mandate (i.e., does it constitute a measure that would ensure continuity of services)?).

## The specialness of the user base

18. Article 68(9) of MiCA requires CASPs to keep records of all crypto-asset services, activities, orders, and transactions undertaken by them. Those records shall be sufficient to enable competent authorities to fulfil their supervisory tasks and to take enforcement measures, and in particular to ascertain whether crypto-asset service providers have complied with all obligations including those with respect to clients or prospective clients and to the integrity of the market.
19. In order to perform their surveillance duties, national competent authorities must be able to identify clients in a unique and consistent manner. Concerning clients that are eligible for a Legal Entity Identifier (LEI), similar to the requirements for investment firms reporting under MiFIR, ESMA considers that also CASPs should have appropriate arrangements in place in order to collect and verify the LEI of its client before the transaction takes place. Concerning clients that are not eligible for a LEI, ESMA considers that also in this instance the same identification methods as the ones imposed on investment firms authorised under MiFID should be applied. In particular, MiFIR prescribes a list of national identifiers, which are dependent on the client's nationality in accordance with a specific methodology for selection and assignment. ESMA considers that the same list should be used under MiCA because firm-specific codes to identify clients/buyer/sellers do not provide for a sufficiently unified and robust identification of natural persons, neither will this ensure the desired uniqueness of natural persons' identification.
20. The SMSG supports the proposal to rely on the methods for client identification that are used under MiFIR<sup>49</sup>, having considered that the expected user base of crypto services may be largely represented by natural persons, not acting in a business capacity, who are not eligible for a LEI. The SMSG also highlights that the special composition of the users' base of crypto services deserves careful attention with regard to the communication methods used to reach crypto users.

## Pre-trade transparency for AMMs in DEX context

21. ESMA builds upon the existing MiFIR rules to develop the MiCA transparency framework, having considered the important similarities between centralized exchanges (CEXs) and traditional exchanges. Therefore, in line with the requirements for financial instruments under MiFIR, ESMA proposes to use the type of trading system as a starting point for determining the appropriate level of pre-trade transparency which must be made public.
22. In its draft RTS, ESMA therefore proposes to calibrate the transparency requirements taking into consideration the different types of trading systems. To that effect, the draft

---

<sup>49</sup> See Section 6.2.4 of the consultation paper (Data elements to be included in the records of all CASPs (Article 68 of MiCA)) and Q50 (Do you anticipate practical issues in the implementation of the methods for client identification that are used under MiFIR?).

RTS therefore includes in Table 1 of Annex I the description, and the related pre-trade transparency requirements, for continuous auction order books as well as other types of trading systems which can also be relevant to the trading of crypto-assets (i.e., quote-driven, periodic auction, and hybrid).

23. In addition, considering the importance and innovative nature of Automated Market Makers (AMMs) particularly in a Decentralised Exchange (DEX) context, ESMA proposes to include a description and the related pre-trade transparency requirements for these trading facilities in Table 1 of Annex I of the draft RTS. AMMs are described as a decentralised protocol relying on liquidity pools and smart contracts which allows the execution of individual transactions in a permissionless and automatic way. As for the information to be made public on operating rules for trading platforms required by Article 1 of the draft RTS, Table 1 of Annex I indicates the mathematical equation used to determine the price and the quantity of the crypto-assets in the liquidity pools and any further information and parameters that allow to determine the price at which a specific order would be executed.
24. The SMSG supports the proposal to require the publication of the mathematical equation used to determine the price and the quantity of the asset in the liquidity pools<sup>50</sup>, as this requirement makes market participants aware of the price setting rule. In this respect, it should be noted that the price discovery function with AMMs differs from the standard one: instead of finding the equilibrium price through the minimization of the order imbalance between buy and sell orders, AMMs determine the price algorithmically through a conservation function (the most common being the “constant product function”). The meaning of ‘price’ with AMMs is therefore different from the usual one. Consequently, the SMSG suggests to disclose not only the mathematical function but also the difference that such function would imply in comparison with more widely known methods to set the price.

## White paper

25. MiCA Regulation – as highlighted by paragraph 228 of the Consultation Paper – explicitly indicates that the purpose of white papers is to inform prospective holders and in particular retail holders of the characteristics, functions and risks of the crypto-assets that they intend to purchase. Recital 24 of MiCA states that – to ensure their protection – prospective retail holders of crypto-assets should be informed of the characteristics, functions and risks of the crypto-assets that they intend to purchase. In particular, when making an offer to the public of crypto-assets other than asset-referenced tokens or e-money tokens (henceforth “other cryptos”), offerors should draw up, notify to their

---

<sup>50</sup> See Section 5.2.1 of the consultation paper (Pre-trade transparency) and Q23 (Regarding more specifically AMMs, do you agree with the definition included in Table 1 of Annex I of the draft RTS? What specific information other than the mathematical equation used to determine the price and the quantity of the asset in the liquidity pools would be appropriate to be published to allow a market participant to define the price of the assets offered in the liquidity pool?).

competent authority and publish an information document containing mandatory disclosures ('a crypto-asset white paper').

26. The white paper should consequently be an "information document", aimed at ensuring the protection of perspective retail holders in particular. Article 6 and Annexes I to III<sup>51</sup> of MiCA establish content and form of crypto-asset white papers. A crypto-asset white paper should contain general information on the issuer, the offeror and the project to be carried out with the capital raised, on the rights and obligations attached to the crypto-assets, on the underlying technology used for such crypto-assets and on the related risks.
27. In this respect Annex II of the draft ITS on crypto-asset white papers establishes formats and disclosure templates for the white papers. In particular, Table 2 contains the templates for other cryptos white papers and item D.10 – included in the part of the white paper providing information about the crypto-asset project – concerns indeed the planned use of collected funds. The SMSG observes that the white paper is published at the issuance of crypto assets and requires to disclose the expected use of funds. The SMSG believes that investors also need to know the actual use of the funds after the issuance (not only the expected use at the time of the white paper).
28. Recital 48 of MiCA states that – in addition to the information provided in the crypto-asset white paper – issuers of asset-referenced tokens should also provide holders of such tokens with information on an ongoing basis. In particular, Article 30 of MiCA requires the issuers of asset-referenced tokens to disclose on their website – and update at least on a monthly basis – the amount of asset-referenced tokens in circulation and the value and composition of the reserve assets<sup>52</sup>. The SMSG highlights the need to provide ongoing information to the holders of other cryptos (not only to the holders of asset-referenced tokens).
29. As regards the format of the white papers, ESMA considers that iXBRL is the machine-readable format that would best meet the legal requirements and policy objectives set out in MiCA and ensure the highest level of consistency with other disclosure requirements for sustainability information. ESMA also observes that the expected cost and effort associated to the preparation of a white paper in the proposed iXBRL format would be very limited<sup>53</sup>. In this respect ESMA considers a MiCA white paper structured as a standalone iXBRL file with a simple "closed" taxonomy (i.e., a template).

---

<sup>51</sup> Annex I lists items to be disclosed in the crypto-asset white paper for other crypto assets, Annex II lists items to be disclosed in the crypto-asset white paper for an asset-referenced token, and Annex III lists items to be disclosed in the crypto-asset white paper for an e-money token.

<sup>52</sup> Article 30(3) of MiCA requires that issuers of asset-referenced tokens should also disclose any event that has or is likely to have a significant impact on the value of the asset-referenced tokens or on the reserve assets, irrespective of whether such crypto assets are admitted to trading.

<sup>53</sup> The costs that issuers or CASPs will face to source the information required by the MiCA Regulation for the white paper are not included in the estimates reported in the consultation paper.

30. The SMSG supports the proposal to use a “closed” taxonomy for the white papers<sup>54</sup>, having considered that such a format would reduce costs and also allow greater comparability across crypto-assets, with positive implications for the information set available to prospective holders.

---

<sup>54</sup> See Section 7.1 of the consultation paper (Standard forms, formats and templates of the white papers), Q57 (Do you agree with the criteria proposed for identifying a relevant machine-readable format for the MiCA white paper and consequently with the proposal to mandate iXBRL as the machine-readable format for MiCA white papers, subject to the outcome of the study referred to in paragraph 239?) and Q58 (If yes, do you agree that the white paper should be required to be a stand-alone document with a closed taxonomy (i.e., without extensions nor complex filing rules)?).

### 8.3 Annex III: Feedback on the Consultation Paper (question-by-question)

#### **Q1: Do you agree with ESMA's assessment of the mandate for sustainability disclosures under MiCA?**

1. Beyond general introductions and forewords on arguments specified in the next questions, respondents agreed overall on the assessment of the mandate.
2. A few remarks warranting further consideration include suggestions to:
  - i. exempt from sustainability disclosures CASPs providing only a specific sub-set of crypto-asset services, e.g. custody services;
  - ii. introduce a 'grace/transitional period' in light of challenges on data availability and quality
  - iii. in cases of multi-layered infrastructures, mandate disclosure on sustainability impacts only at the level of the DLT systems of layer 1 blockchains, where information would be more readily available.

#### **Q2: In your view, what features of the consensus mechanisms are relevant to assess their sustainability impacts, and what type of information can be obtained in relation to each DLT network node?**

3. A few respondents called for ESMA to specify the different types of consensus mechanisms as a common taxonomy underpinning the assessment of sustainability impacts. Other respondents provided a long list of types of consensus mechanisms, noting it will likely evolve in the future.
4. Some respondents challenged the scope of the RTS and the definition of DLT network node: they noted that it will be impossible to identify all the nodes for larger and more decentralised networks (e.g. Bitcoin), and called for distinguishing between nodes with different functions (e.g. validating nodes) and for clarifying whether miners will be in scope. A large number of respondents expressed caution on the use of location of DLT network nodes.
5. In line with responses in other questions, a large part of individual respondents advocated for taking into account the presumed positive impacts of the consensus mechanisms. A few respondents also noted that sustainability impacts linked to the security and resilience of the consensus mechanisms are necessary to their well-functioning.

#### **Q3: Do you agree with ESMA's approach to ensure coherence, complementarity, consistency and proportionality?**

6. While welcoming ESMA's overall approach, most respondents called for further clarifications or adaptations of the draft RTS, notably for consistency and proportionality.
7. Some respondents asked additional guidance on what constitutes 'limited data availability' that would trigger the best efforts clause and the use of estimates, with others indicated that this proposed 'best efforts' approach already sets a high bar.
8. In line with responses to Q10, a few respondents advocated for more guidance on the '*information distribution model*', stating that CASPs may only disclose information previously made available in white papers and that their liability for such information should be limited. A few respondents challenged the requirements to review the information regularly and at least annually.
9. In line with responses to Q6 and Q7, a large part of respondents (notably individual respondents) lamented the focus on adverse sustainability impacts and suggested to include indicators on the positive impact on consensus mechanisms, on the use of DLT network nodes and/or on the projects financed thanks to crypto-assets.
10. Some respondents favoured the inclusion of de minimis thresholds (e.g. based on issuance size for ARTs and EMTs) under which issuers and/or CASPs should not be required to disclose information on sustainability impacts.

**Q4: Do you agree with ESMA's approach to mitigating challenges related to data availability and reliability? Do you support the use of estimates in case of limited data availability, for example when data is not available for the entirety of a calendar year?**

11. The vast majority of respondents expressed a strong support for the use of estimates, while a few respondents note that using estimates in case of low data availabilities may be counterproductive. Other respondents call for the use of estimates only for cryptos issued after the application of MiCA and/or for a limited period.
12. One respondent suggested that ESMA and/or NCAs provide the estimates themselves or publish an indicative 'white-list' of providers of sustainability data deemed reliable.
13. Some respondents ask for additional guidance on some concepts (inspired from the existing sustainable finance), including on the notion of 'best efforts' and on what constitutes 'reasonable assumptions' in article 4(8).
14. One respondent drew a parallel with the existing framework for financial reporting, calling for clarifications on whether audit and/or assurances from third parties would be mandated.
16. In line with their responses in other questions, a few respondents call for reducing reporting requirements for CASPs, notably by limiting the data they have to provide to the sustainability indicators reported in white papers.

**Q5: What are your views on the feasibility and costs of accessing data required to compute the sustainability metrics included in the draft RTS?**



17. Responses were rather varied with regards to their impression of the cost and feasibility of the proposals. While some respondents indicated concern with regards to the difficulty to obtain high quality data, of needing to outsource data collection, of the cost of using third party providers, most were satisfied with the possibility of using estimates, while noting that this would involve costs as well (and wondering whether a golden /whitelist source could be provided, or at least a greenlighted methodology to avoid incoherent results across data providers / greenwashing, if not forbearance). A few respondents also noted that in their view the proposal was rather feasible, and that on the short run this might involve a market for data while on the long run entities would develop their own data collection abilities. One respondent tested the mandatory requirements and found that they were able to provide disclosures for 27 crypto assets so far.
18. Several respondents suggested a need to differentiate between responsibilities of issuers and those of CASPs, noting that the responsibility for disclosures should lie with issuers rather than CASPs (but in some cases acknowledging that the mandate covers CASPs).
19. Other respondents supported flexibility and proportionality depending on the size of the relevant entities. One respondent noted the low disclosure threshold and wondered whether entities of a value and market share below a certain amount might be exempted from these requirements.
20. Finally, a few respondents provided feedback and suggestions with regards to individual proposed indicators, namely requesting optional indicators providing disclosing entities with an opportunity to disclose positive results.

**Q6: Do you agree with ESMA's description on the practical approach to assessing the sustainability impacts of consensus mechanisms? If not, what alternative approach would you consider suitable to assess these impacts?**

21. Responses to this question were varied in nature and views.
22. First, more generally, some agreed with ESMA's approach, noting that the approach may not fully highlight certain positive environmental aspects of PoW consensus. Some supported a stepped approach, focusing on short, medium, and long-term aspiration taking into account the operational challenges at hand.
23. Some respondents expressed concerns with (ESMA's understanding of) the scope of the RTS mandate, with some expressing concern with the mandate's sole focus on the sustainability of the infrastructure, rather than that of the issuer (and some simply stating an absence of link between consensus mechanisms and sustainability impact), others questioning the focus on environmental, rather than ESG impacts, and finally some noting a discrepancy between the focus on adverse impacts found in MiCA and the more general (positive and negative) analysis of sustainability impacts found in other legislation.
24. Furthermore, a few fundamental points raised concerned how to ensure comparability of results and suggesting an urgent need for a harmonised definition and methodology

for the calculation of indicators, proposals for a phased approach starting with indicators for which there is the highest level of data availability and data quality, whether thresholds might be applied to ensure proportionality for small issuers / CASPs with limited risk of adverse impact or to ensure feasibility by setting an acceptable level of data coverage (e.g. 80% of nodes), and finally whether CASPs should have responsibility for the accuracy of these requirements and whether they should even apply to CASPs not operating trading platforms.

25. In addition, some respondents noted the limitations in data access given the difficulty of identifying the location of nodes due to the use of VPNs and the frequent location of nodes outside the EU. One respondent suggested that in practice under Bitcoin blockchains what matters is the sustainability impact of AWS, while under Ethereum blockchains it is the sustainability impact of Solana.
26. Finally, more specifically, one respondent noted the importance of separately considering the energy consumption of a transaction and that of the maintenance of the blockchain, while another noted that energy shouldn't be measured per transaction but per block, some suggested that a (semi-)decentralised player couldn't have targets, and one noted the need for practical examples in the RTS of how to use these disclosures so as to avoid misleading investors.

**Q7: Do you agree with the definitions proposed in the draft RTS, in particular on incentive structure and on DLT GHG emissions? If not, what alternative wording would you consider appropriate?**

27. Most respondents responded positively, with many offering similar responses.
28. A number of respondents noted the importance of maintaining simplicity in the requirements and coherence across borders given the cross-border nature of the market (suggesting requirements only be made more precise at a later stage). One respondent noted the importance of having a methodology.
29. Some noted that Scope 3 requirements, while not harmful, might be unnecessary, while others noted that participation in PoW often had other focuses than validating transactions, and that we should therefore instead just refer to achieving agreement as the objective.
30. Finally, a group of respondents noted the positive environmental impacts of PoW and expressed fears that the requirements might lead to a negative bias on the net impact of PoW whereas they might have a specific positive impact on the environment.
31. One respondent noted that the requirements should apply miner by miner rather than on the entirety of the network and only those in jurisdictions covered by MICA.
32. One respondent noted their view that the scope of the mandate was less wide than ESMA's understanding.

**Q8: In your view, are the proposed mandatory sustainability indicators conducive to investor awareness? If not, what additional or alternative indicators would you consider relevant?**

33. Respondents' views with regards to whether the proposed mandatory sustainability indicators are conducive to investor awareness were rather varied.
34. Some considered that the proposed indicators provide an appropriate and quantifiable measure of sustainability performance, in particular referring to energy consumption and greenhouse gas (GHG) emissions, and that they are consistent with those in traditional finance – and proposed additional specifications to ensure comparability.
35. At the same time, others expressed concerns with regards to the amount and complexity of proposed indicators, the availability and quality of data, and to whether the indicators would genuinely affect investor decisions (and in terms of specific indicators, some noted that energy consumption and intensity were not representative of sustainability, others noted that CASPs should not have to report Scope 1 and 2 GHG emissions and should instead report Scope 3 GHG emissions).
36. While acknowledging the advantages of estimates, some respondents noted the risk these might create in terms of comparability between disclosures, and therefore favoured starting with a limited set of mandatory indicators understandable to investors and for which data (and where necessary associated estimation methods) is available through market-approved sources of information, and the development of international standards and methodologies (some asking that ESMA or another entity create standards to be used across the industry, and develop and publish sustainability estimates tailored to blockchain technology to ensure CASPs can incorporate reliable and standardised sustainability metric to comply with their obligations)).
37. Some respondents noted the importance of making investors aware of the limitations in terms of data availability and quality – in particular as regards the necessary approximations of node location and energy mix – and suggested that ESMA should clarify what factors are taken into account to assess an indicator's conduciveness to investor awareness.
38. In addition, some respondents suggested that the indicators should be accompanied by some clearly defined perspective, for example through the development of an energy label (or in some cases comparisons to non-industry benchmarks or information on how these disclosures should work in practice for different types of crypto assets), while others noted the risks associated with the information being available on each CASP's website leading to inconsistencies and limitations to investor awareness (several respondents noted opposition with CASPs – and especially those not operating trading platforms – being responsible for the data).
39. Finally, some respondents expressed disappointment with the focus on adverse impacts, meaning entities do not have a specific opportunity to present the positive environmental impacts specific to PoW – which they consider not conducive to investor awareness,

while others disagreed with ESMA's interpretation of the scope of the mandate, and some suggested a minimum threshold of application of these requirements.

**Q9: Do you consider the proposed optional sustainability indicators fit for purpose? If not, what additional indicators would you consider relevant? Would you agree to making these optional sustainability indicators mandatory in the medium run?**

40. Respondents provided their feedback with divergent orientations.
41. A fraction showed support for the proposal of making optional indicators mandatory in the medium run. One also suggested a phased approach to consider the burden for entities. Other respondents asked that a post-implementation review be conducted before changing optional indicators into mandatory. One also suggested that optional indicators should be open to be filled with metrics available to operators.
42. Another part would keep the indicators as optional and suggests focusing on consistency and clarity of limited mandatory indicators, with expansion of the optional ones. Additional indicators suggested were: renewable energy consumption; positive impact indicators; second order effect; size of CASPs. One respondent also states that energy consumption and energy intensity should fall in the optional indicators as they are not a accurate measure.
43. Finally, some respondents are against the optional indicators and support only the implementation of the mandatory ones. One in particular proposed a simpler traffic light approach. Another stated that node consumption is not a good approximation as nodes are not necessarily the main sources of environmental impact for blockchains.
44. A general comment was that these indicators should be clearly defined as 'optional' in the RTS, instead of 'additional'.

**Q10: Do you consider the principles for the presentation of the information, and the template for sustainability disclosures fit for purpose? If not, what improvements would you suggest?**

45. Respondents provided different suggestions for improving the proposed template.

Some suggest amending Article 4 and annex of the RTS considering the 4 different scenarios with respect to the issuance of white papers: 1) An EU/EEA issuer which issues a white paper: CASPs should provide only 'General information and key indicators' in Table 1; 2) An EU/EEA issuer not issuing a white paper: CASP should benefit from an exemption from the disclosure obligation; 3) A third country issuer issuing a white paper: same as 1; 4) A third country issuer issuing a white paper that is not in line with the MiCA requirements, or not issuing a white paper, or there is no issuer: full application of Article 66(5) obligation to provide sustainability related information, just for CASPs that operate a trading platform. Other proposals are:

- i. Add an executive summary field for context;

- ii. Include field for positive impact and qualitative information ;
  - iii. Avoid splitting carbon emissions into scopes to avoid confusion;
  - iv. Introduce ranges and colour coding;
  - v. Add keys to facilitate comparison of data between CASPs;
  - vi. Introduce a 'lite' regime for SMEs and start-ups;
  - vii. Ensure machine-readability.
46. Some respondents highlighted the high level of subjectivity in the different columns of the template, implying low comparability. One asked for further clarifications on i) the relevant elements that contribute to the comparison of data between several CASPs, ii) the allocation of responsibilities among various CASPs, and iii) responsibilities of CASP and issuer. Another requested clarification on which entities are being compared in the presentation of the impact on the climate of each consensus mechanism used, as under Art. 3(3).

**Q11: In your view, are the calculation guidance for energy use and GHG emissions included in the draft European Sustainability Reporting Standards relevant for methodologies in relation to the sustainability indicators under MiCA? If not, what alternative methodologies would you consider relevant? For the other indicators for which the calculation guidance of the ESRS was not available, do you consider that there are alternative methodologies that could be used? If so, which ones?**

47. Some respondents find the ESRS to be a good initial framework but underscore the uniqueness of crypto assets and the need for further clarifications from ESMA. Many respondents didn't show support for the use of the ESRS; a common concern is that the ESRS are still new also for CSDR firms, and that they may bring additional challenges for MiCA entities.
48. Other methodology proposals are:
- i. CCRI/Southpole as a main example of CA-specific methodology;
  - ii. Multi-step approach: first await the outcomes of ESMA tender on 'Developing a Methodology and Sustainability Standards for Mitigating the Environmental Impact of Crypto assets' to gain industry insights and develop specific procedures; then, start a test phase to determine the relevant criteria;
  - iii. Decentralised approach through more self-reporting and third-party audit for energy-related data;
  - iv. Issuer-centric approach based on SFDR;

- v. Dual reporting from carbon accounting: location-based accounting (required) and market-based accounting (optional).

49. Overall, there are two different views on the guidance to be provided:

- i. There is a need for a standardised framework to ensure transparency and comparability;
- ii. Reporting needs to be more flexible and decentralised to avoid regulatory burdens, since comparability cannot be ensured in any case.

**Q12: Would you consider it useful that ESMA provides further clarity and guidance on methodologies and on recommended data sources? If yes, what are your suggestions in this regard?**

50. All respondents agree that further guidance on the methodologies is needed. The suggestions are:

- i. Engage with industry experts and researchers;
- ii. Create a whitelist of reliable data sources like blockchain-based data or oracles;
- iii. Give standardised methodologies for calculating energy consumption, greenhouse gas emissions, and electronic waste, with regular updates;
- iv. Outline best practices;
- v. Guidelines that allow for flexibility;
- vi. Clarify whether issuers and CASPs should disclose distinct metrics;
- vii. Encourage collaboration between issuers and CASPs ;
- viii. Encourage collaboration with EU and international relevant stakeholders;
- ix. Run pilot programs;
- x. Set up a consensus database to tackle the lack of data;
- xi. More precision in the definition of permissionless DLT;
- xii. Review and consultation after the first application phase of the RTS.

51. The general plea is to design guidelines which balance offering specific guidance and prescription with allowing for flexibility. Two respondents also warned about the lack of objectivity of industry researchers, regarding the recommended data sources.

**Q13: Is the definition for permissionless DLT in Article 1 sufficiently precise?**

52. Most respondents said the proposed definition of permissionless DLT in the draft RTS required further clarification. The main concern was whether the definition would subject CASPs to greater liability than intended in Level 1 as it relates to the use of permissionless DLTs in their services as well as the reference to the clause in the definition: "...in which no entity...provides *core services* for the use of such distributed ledger".
53. Several respondents argued that there should be no distinction between liability for permissionless and permissioned DLT, rather, the test should be whether the CASP has effective control of the DLT (in which case it would be liable for client losses). By contrast, another respondent called for an additional definition of 'permissioned DLT' with which to compare 'permissionless' against.
54. One respondent called for a clear distinction to be made between the fully decentralised 'ecosystem' and the 'distributed ledger service layer' only. The addition of the notion of a 'free entry point' in the definition would be of help in making this distinction. Whereas another respondent argued that the notions of 'permissions' and 'centralisation' of the DLT were conflated in the proposed definition.
55. Several respondents addressed the concept of 'core services' in the definition, arguing that a CASP may interact with a DLT platform in different ways and may provide core services without having control of the DLT. As such, they argued that this clause should be removed from the definition. Clarify that the term "entity" in this definition does not refer to public bodies or state actors, to allow for a combination of permissioned and permissionless elements.
56. One respondent proposed development of further Level 3 guidelines on this concept because of the highly diverse nature of DLTs which may have hybrid structures in which the permissionless/permissioned nature of the network must be understood at the level of analysis of each layer (application, consensus, node, etc).
57. Several crypto native respondents opposed the introduction of a formulation of 'permissionless DLT' that was narrower than how it is understood by the industry. Another respondent noted that the definition does not match exactly those developed by the FSB or the ESMA Guidelines on standard forms, formats and templates to apply for permission to operate a DLT Market Infrastructure (ESMA70-460-206).

**Q14: Throughout the RTS, we refer to 'critical or important functions.' The term is borrowed from DORA and does not just capture ICT-specific systems. Does this approach make sense?**

58. There was a general consensus among respondents that borrowing of the term, 'critical and important functions' from DORA would be ideal for promoting consistency between EU financial regulations. Indeed, there was strong support from most respondents across the industry spectrum (crypto native and traditional finance) who agreed with the approach of not duplicating / overlapping with the DORA requirements and maintaining definitions in common. The only caveat was as it relates to ensuring that CASPs are able



to identify their own critical or important functions in line with the principle of proportionality, with guidance from the ESAs and/or relevant NCAs (if necessary).

59. One respondent noted that offerors and persons seeking admission to trading of crypto-assets other than ART and EMT would not be subject to the ICT-specific provisions of DORA since they are not considered 'financial entities' under that regulation.
60. Of the respondents who objected, the chief concern was the 'wide scope' of the terminology. In fact, two respondents noted that the term 'critical or important functions' entered into the DORA lexicon from Article 2(1), point (35) of Directive 2014/59/EU (BRRD)<sup>55</sup>. Hence, they advocated for using the BRRD definition instead.

**Q15: Do you consider subparagraph (e) in Article 4(2) on external communications with clients in the event of a disruption involving a permissionless DLT appropriate for the mandate (i.e., does it constitute a measure that would ensure continuity of services)?**

61. Most respondents supported the obligation for the CASP business continuity plans to include measures for external communications with clients in the event of a disruption to a permissionless DLT (with some caveats about how to operationalise the obligation). Others argued that the provision did not constitute a measure to ensure business continuity. Even those who opposed it in principle offered additional clarifications or proposals to retain the investor protection aspects in a more practicable manner for CASPs.
62. Most respondents noted the importance of maintaining in the RTS an understanding that the CASPs should only be accountable for their *own services* that use the DLT, not the *underlying DLT infrastructure* itself. Given that the requirement relates to updates about the DLT infrastructure and *not the availability of CASP services*, there is some information that CASPs would not have access to at a given moment. Therefore, some respondents said, point (e) should be reframed to ensure such communication should be made to the best of the CASPs ability and in accordance with their clients' best interests.
63. Relatedly, one respondent said CASPs should, when communicating externally, 1) clarify the *significance* of the impact and 2) ensure *precise information*. Otherwise, there is a risk of 'noise' interfering with the ability of consumers to differentiate between 'inconsequential' and 'severe' disruptions. Another respondent built on the idea of *significance* of the impact of the incident by calling for the requirement to be linked only to those incidents identified as 'major' per the incident reporting classification in the DORA regulation.

---

<sup>55</sup> 'Critical functions' as in Article 2(1) of [Directive 2014/59/EU](#) of the European Parliament and of the Council of 15 May 2014: "critical functions' means activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of an institution or group, with particular regard to the substitutability of those activities, services or operations."

64. Those who objected to the provision said that since the CASP may not ultimately be in a position to provide the most accurate or timely information about the nature of the disruption of the DLT or when it may come back online, it should instead prioritise reasonable measures to secure the property of its clients and provide updates to clients on the situation as it evolves at reasonable intervals.
65. Another respondent asked for clarification about whether this ‘timely external communication’ measure would also apply to a CASP’s permissioned (or owned and operated) ledgers and whether these types of DLT infrastructures would meet the standard of a ‘critical or important function’ for the purpose of the business continuity plans.

**Q16: Should this RTS also specify that CASPs should establish a business continuity management function (to oversee the obligations in the RTS)? In your view, does this fall within the mandate of ‘measures’ ensuring continuity and regularity?**

66. Several respondents expressed concern that a requirement to establish a business continuity management function would, in some cases, create a disproportionate burden. Respondents thus highlighted the importance of a proportional application of the requirement to have a dedicated continuity management function. In this light, there were suggestions to exempt microenterprises or apply it only to significant CASPs. Overall, there was relative consensus amongst respondents that resources need to be dedicated to business continuity but that a specific business continuity management function would not, in all cases, be needed. Respondents stated that the level of resources dedicated and the specific form in which they are dedicated should be subject to some flexibility and proportionality.

**Q17: Are there other organisational measures to be considered for specific CASP services?**

67. Most respondents stated that the organisational measures in the RTS are sufficient and there is no need to consider additional ones. The main arguments given are that the current requirements seem sufficient to ensure business continuity and that further requirements would place too high a burden on CASPs.
68. One respondent asked to focus on organizational measures that address the risks specific to providing crypto asset services. Another respondent identified the need for organizational requirements specific to CASPs who rely on third parties for their digital asset custody services (custody technology service providers). This respondent argued there should be rules and standards for CASPs in selecting such third parties.

**Q18: Do you consider the obligation for CASPs to conduct testing of the business continuity plans in Article 4(4) via an internal audit function appropriate for the mandate?**

69. Most respondents found the proposal to be adequate, as it is common industry practice, and it ensures internal accountability between the CASP’s management body and its functional areas responsible for execution of the business continuity policy. Some

respondents advocated for the possibility to have an external auditor, which would be preferable for smaller or non-group (standalone) CASP entities.

70. One respondent underscored that testing of business continuity plans for scenarios involving a permissionless DLT would require a complex, multi-party strategy. Another respondent suggests introducing a transition period for the obligation of one year and then requiring the audit every two years.

**Q19: In Art. 68(8), CASPs are required to take into account the scale, nature, and range of crypto asset services in their internal risk assessments. Is there support for this general principle on proportionality in Article 6? Do you support the proposed self-assessment under Article 6(2) and in the Annex of the draft RTS?**

71. Most respondents supported the self-assessment. Specific comments included:
- i. Two respondents suggested the addition of a criterion for the type of assets that are held in custody (in part (b) of the Annex), considering the variance in volatility between assets.
  - ii. One respondent proposed the inclusion of ESG criteria and scale of personal data collection in the self-assessment.
  - iii. One respondent called for a reference to Art. 68(8) directly in the article. Another proposal called for extending the self-assessment minimum timeframe be extended to at least every two years so as not to inflict ‘unnecessary burden.’
  - iv. Changes in Point C, subpoint (v) and (vi), which are not applicable to all CASPs:
    - a. Remove sub-point (v) and edit (vi) in “how the private cryptographic keys or other means of accessing crypto-assets of clients are secured under safekeeping”;
    - b. Add clarification note on where criteria are not applicable and how it will be treated;
    - c. Add the term “if any” at the end of the subpoints.
72. Only one respondent objected to the self-assessment (but supported the proportionality principle). They reasoned that the self-assessment would be duplicative to the obligations in their business continuity plans and urged the RTS to allow CASPs to choose their own criteria for the self-assessment.

**Q20: Do you agree with the description provided for the different types of CEX and DEX listed?**

73. The feedback from the 23 respondents that provided a view regarding the definitions and descriptions of CEXs and DEXs support ESMA’s approach , with some respondents offering detailed feedback or suggestions for improvement.
74. The main suggestions for clarification include (i) the accurate representation of how CEXs and DEXs operate, (ii) the treatment of decentralised finance, and (iii) the potential for emerging hybrid models that could challenge existing classifications.

75. Several respondents called for more precise language, particularly around the settlement processes for CEXs and the operational nature of DEXs, including their governance through smart contracts and the lack of a central operator.
76. The unique aspects of DEXs, such as their contribution to financial inclusivity and autonomy, were highlighted by some respondents as important. Respondents also raised some concerns in relation to the scope of MiCA and the regulatory treatment of fully decentralised services without intermediaries.

**Q21: For trading platforms: Please provide an explanation of (i) the trading systems you offer to your users, (ii) which type of orders can be entered within each of these trading systems and (iii) whether you consider these trading systems to be a CEX or a DEX (please explain why)?**

77. Respondents indicate a diversity of trading systems used in crypto-assets trading platforms. Responses indicate a variety of trading systems in use, including central limit order books (CLOB) and continuous auction order books, with a primary focus on centralised trading platforms.
78. In relation to order types, the feedback received from respondents indicate a wide range of order types, including market, limit, stop limit, and more sophisticated orders like OCO (one cancels the other) and TIF (time in force) conditions, highlighting the advanced trading functionalities provided to users.
79. Most respondents classify their trading systems as CEX due to centralized management of order books and matching algorithms. However, there's an acknowledgment of the complexity in categorizing platforms that utilize DEX systems for proprietary trading or sourcing crypto.
80. Finally respondents emphasised on the need for clear differentiation between truly decentralised platforms (DEX) and those that, while utilizing decentralized technologies, are operated by identifiable entities and should comply with CEX obligations.

**Q22: Do you consider the trading systems described, and the transparency obligations attached to each trading system, in Table 1 of Annex I of the draft RTS appropriate for the trading of crypto-assets? Do you offer a trading system that cannot meet the transparency requirements under the provisions in this Table? Please provide reasons for your answers.**

81. Most respondents consider the types of trading systems listed in Table 1 of Annex 1 of the draft RTS sufficient to capture the models used in crypto-asset trading. Respondents noted that they currently use at least one type of system listed, with the most commonly cited being the continuous auction order book. In addition, several respondents noted that they already make available to the public the aggregated numbers of orders and the crypto-assets they represent at each price level for more than the five best bid and offer price levels.

82. One respondent (a trade association) was neutral on the basis that the MiFIR principles from which the transparency obligations draw inspiration may not correspond perfectly to the market for crypto-assets. In their objection, this respondent used the hypothetical of a (blind) NFT auction in which pre-trade transparency would not be possible. Hence, they argued that pre-trade information should not always be an obligation whereas post-trade information should always be mandatory.
83. One respondent objected to some aspects of the systems listed in Table 1 and proposed requirements on operators of CLOB trading systems to make their entire order book public (instead of 'at least' the five BBO) – the respondent justifies this suggestion as in their view could help with the prevention of market abuse. This same respondent also asked for clarity on MiCA's treatment of matched principal trading and whether it would be captured as an activity conducted by trading platforms for crypto-assets. Finally, the respondent noted that liquidity provision in an AMM context can be equated to 'dealing on own account' which is not covered by the MiCA framework.
84. Another respondent proposed extensions or modifications of the text in Table 1. The respondent suggested the addition of a disclaimer to say that AMM systems would only be applicable in scope of MiCA when operated by a CASP. The same respondent also proposed new drafting for the description of how AMMs work and the pre-trade information that should be made public, including the level of liquidity in the pool at a given moment which would be a requisite for calculating price on a continuous basis.

**Q23: Regarding more specifically AMMs, do you agree with the definition included in Table 1 of Annex I of the draft RTS? What specific information other than the mathematical equation used to determine the price and the quantity of the asset in the liquidity pools would be appropriate to be published to allow a market participant to define the price of the assets offered in the liquidity pool?**

85. One respondent called for the term 'automated market maker' (AMM) to be defined in the RTS, not just in the Annex. Several respondents pointed to drafting errors in Recital 5 (and proposed alignment with the description of AMMs in the Annex). The same respondents argued that Article 2(1) of the RTS conflates 'trading systems' with 'trading platforms'.
86. Several respondents argued that smart-contract AMMs should not be in scope as they constitute 'decentralised activities'. Another respondent confirmed view that only AMMs owned and operated by CASPs should be in scope of this Regulation.
87. According to one respondent, some AMMs allow the exchange of crypto-assets in a permissionless manner, but the provision of liquidity, which may be classified as transfer of crypto-assets, is often permissioned. In other words, certain AMM protocols do not allow any and every user interacting with the protocol to create a liquidity pool of supported tokens. Therefore, this respondent argued, the definition should be amended to reflect this.

88. Several respondents said disclosures of the number of liquidity providers (and their share of liquidity-provider token holdings in each pool), should be considered as an addition to pre-trade information as it could help investors assess the risk and health of that pool. For the CLOB model, another respondent said information regarding health of the order book can be derived from disclosure in field 12 of pre-trade transparency report.
89. One respondent suggested some additional transparency options, including transaction (or 'swap') fees, pool token supply (to assess risk and health of the pool), and reserve balances (of each crypto-asset in the pair), and slippage.

**Q24: Do you agree with ESMA's proposals on the description of the pre-trade information to be disclosed (content of pre-trade information) under Table 2 of Annex I of the draft RTS? If not, please explain why. If yes, please clarify whether any elements should be amended, added and/or removed.**

90. Almost all respondents that provided a view on the proposal to standardise the information to be provided agreed with ESMA.
91. Nevertheless, some respondents suggested adding some fields:
- i. blockchain / token standard;
  - ii. DTIF ticker: short name that is in the process of being created in a standardised manner by the DTIF.
92. Another respondent suggested to remove three fields:
- i. venue and trading system;
  - ii. quantity currency, price currency and price notation;
  - iii. number of orders and quotes.
93. Only one respondent was against the proposal – suggesting keeping the flexibility given for traditional finance instruments under RTS 1 and 2.

**Q25: Do you agree with ESMA's proposals to require a specific format to further standardise the pre-trade information to be disclosed (format of pre-trade information)? If not, please explain why and how the pre-trade information can be harmonised. If yes, please clarify whether any elements should be amended.**

94. The majority of respondents agreed with ESMA's proposal on the pre-trade information to be disclosed. Nevertheless, some of these respondents noted that this may put high compliance costs to implement the proposed format. This element should be further considered by ESMA, respondents suggest.
95. Those respondents that are against the introduction of harmonisation of pre-trade data suggest that practices between crypto-assets and traditional finance should be aligned.



Therefore, if there are currently no requirements under RTS 1 and 2 to harmonise the format of pre-trade data that should not be introduced to DeFi either.

**Q26: Do you agree with the proposed approach to reserve and stop orders?**

96. All respondents agreed with ESMA's proposed approach to reserve and stop orders. However, some respondents considered that, although noting the legislative constraints, ESMA should consider other exemptions to pre-trade transparency. In particular, these respondents consider that waivers for large orders are crucial for crypto markets.

**Q27: Do you agree with the proposed list of post-trade information that trading platforms in crypto assets should make public in accordance with Tables 1, 2 and 3 of Annex II of the draft RTS? Please provide reasons for your answers.**

97. Respondents agree with ESMA'. However, some respondents made the following suggestions:

- i. information on fees or any other costs associated with the transaction could be relevant. Also, considering the specificities of crypto-assets, data related to the blockchain network, like block confirmation numbers, might enhance the quality of post-trade information.
- ii. the "crypto-asset full name" field seems not necessary since the information of the crypto asset admitted to trading would be complete with the "Crypto-asset identification code" field (field 3).
- iii. consider pushing the timing requirements to [one] minute, so as to be consistent with the requirements under MiFID for the post-trade transparency of equity products.
- iv. we consider that the timing requirements related to making post-trade reports, within 30 seconds after the execution of the transaction may not be achievable at all times since there may be latencies for a variety of reasons outside our control such as increased on-chain volume and delayed block settlement. We would welcome ESMA extending the timing requirements to one minute, so as to be consistent with the requirements under MiFID for the post-trade transparency of equity products.

98. Among those who did not agree with ESMA's approach, one respondent questioned the use of the ISIN and another questioned the inclusion of many fields as it would slow down the performance of data feeds and may not add much to the end user, given that they might be derived from the core data. A respondent suggest the following fields to be disclosed.

- i. Market (e.g. BTC-USD);
- ii. Price (in quote currency), quote currency is derivable from the Market, which is the second half of the Market field. Our asset pairs endpoint (linked below) can also be used for a map of our Market <> base/quote currencies;



- iii. Volume (in base currency), or quantity. For reference, "volume" is more conventionally used in our WebSocket API;
- iv. Side of the transaction (buy/sell);
- v. Type of order (limit or market order).

**Q28: Is the information requested in Table 2 of Annex II of the draft RTS sufficient to identify the traded contract and to compare the reports to the same / similar contracts.**

99. Respondents agree that the information requested is sufficient and all relevant and necessary data is specified.
100. One respondent expressed that FIGI could add extra asset coverage and useful granularity in respect of trading location.

**Q29: Is there any other information, specific to crypto-assets, that should be included in the tables of Annex II of the draft RTS? Please provide reasons for your answers.**

101. In terms of whether any other information should be included, respondents suggested the following:
  - i. to specify the stabilisation mechanism of a crypto-asset, in particular of Asset-Referenced Tokens (“[...] referencing another value or right or a combination thereof, including one or more official currencies”). Important post-trade transparency data as mechanism will have impact on the value of the crypto-asset after it has been sold.
  - ii. to include any information with regard to the type / nature of crypto-asset traded.
  - iii. to include the order-type for post-trade transparency i.e. limit orders, stop-limit orders, market orders, fill-or-kill etc. Large market orders are often executed at various prices as they fill the ask-side of the CLOB. This means that a trader’s singular market order is executed partially at different prices. Post-trade, the trader should be made aware of both the average price of his trade (encompassing all of the sub-transaction executions) and the percentage/quantity of his transaction filled at each price.
  - iv. to include positive impacts on sustainability as well as any negatives.
  - v. to include the FIGI
  - vi. the initial quantity (Field 25 of Table 2 Annex II) allows for a maximum number of 18 digits of which a maximum of 17 fraction digits. This may be insufficient and incur a loss of information, since many assets support a large number of fraction digits - 18 in the case of Ethereum.

- vii. to include specific elements related to crypto-assets to enhance the comprehensiveness of the data such as wallet addresses, smart contract addresses, blockchain identifiers and timestamps. Reporting on such elements can assist in identifying market manipulators or insider traders and better understand the issuance and trading dynamics of these instruments.

**Q30: Do you expect any challenges for trading platforms in crypto assets to obtain the data fields required for publication to comply with pre- and post-trade transparency requirements under Annex I and Annex II of the draft RTS?**

102. Respondents did not foresee any particular challenges for trading platforms in crypto assets to obtain the data fields required for the publication of pre- and post-transparency data. However, some respondents noted that appropriate implementation time should be given for trading platforms to have systems in place to comply with their obligations.
103. Two respondents noted that there may be some challenges in obtaining some data fields, in particular in relation to real-time reporting and blockchain data. They further noted the potential implementation costs, the ability to receive accurate data and raised privacy and security concerns.

**Q31: What do you consider to be the maximum possible delay falling under the definition of “as close to real-time as is technically possible” to publish post-trade information in crypto-assets? Please provide reasons for your answer.**

104. Respondents consider different maximum delays in order to fall under the definition of “as close real-time as is technically possible”, ranging from as long as two hours, 15<sup>1</sup> or 10 minutes.
105. Nevertheless, it should be noted that the vast majority of respondents, despite agreeing that a transaction on a CEX could be published very quickly (i.e. below the thirty seconds proposed by ESMA), they considered that the requirements applicable to crypto-assets should be aligned with traditional instruments (shares in particular) and a one-minute delay should be allowed for cryptos.
106. Respondents note that there may be circumstances, for example due to adverse market conditions or the underlying technology, that justify the alignment with the requirements under MiFIR for traditional assets.
107. One respondent also shared their concerns that the current regime does not allow for a specific delay for large block trades (unlike the CFTC). They urge ESMA to consider allowing for delays depending on the type or size of the transaction.
108. For DEX, the feedback was clear that the time needed is longer than for transaction on-chain given their characteristics. However, only one respondent suggested a timeframe – 24 hours – whilst the majority noted that the timeframe to publish on-chain transactions can vary and the availability of information may not be consistent.

**Q32: Do you agree with ESMA's approach on the requirements to be included in the draft RTS in relation to a trading platform's operating conditions? Please provide reasons for your answer.**

109. The majority of respondents expressed support for ESMA's approach on the requirements to be included in the draft RTS concerning a trading platform's operating conditions.

110. The common theme across these responses is the acknowledgment of the need for transparent, comprehensible, and accessible operating conditions for trading platforms, which align with standards applied to traditional financial trading venues.

**Q33: Do you consider that ESMA should include in the RTS more specific disclosure rules regarding a trading platform's operating conditions, in particular in relation to co-location and access arrangements?**

111. Most respondents do not believe that ESMA should include more specific disclosure rules regarding trading platform operating conditions, particularly concerning co-location and access arrangements.

112. The common sentiment is that flexibility should be maintained, and the existing provisions or general practices under MiFID II are not immediately relevant or necessary for crypto-asset trading platforms at this stage.

**Q34: From your experience, are all crypto-assets trading platforms making their data available free of charge? If not, what specific barriers have you encountered to access the data (e.g., price, level of disaggregation).**

113. Respondents largely agreed that, today, many (if not most) crypto-asset trading platforms offer certain types of market data for free. Data is typically available for prices (OHLC) on crypto-to-crypto or crypto-to-fiat pairs. There was also some variation in terms of granularity, time to publication (i.e., is it real-time?), and the intervals available for historical time series.

114. However, one respondent noted that such market data would likely become a source of revenue for crypto-asset trading platforms in the future as competitive pressures increase. As such, this respondent advocated against regulatory requirements that would restrict the ability of CASPs to monetise their data (there were two specific objections to the ESMA staff views in paragraphs 141-144 of the Consultation Paper).

115. Another respondent said some crypto-asset trading platforms currently charge a fee to access disaggregated data. Here, the price may depend on the profile of the data user: professional or retail.

**Q35: Do you agree with the level of disaggregation proposed in the draft RTS? Please provide reasons for your answer.**

116. Most respondents supported the proposal, confirming that the level of disaggregation proposed in Table 3 of Annex I (pre-trade) and Table 2 of Annex II (post-trade) of the RTS is sufficient to meet transparency requirements. There was also broad support for disaggregation on a crypto-asset by crypto-asset basis as this would be ideal for data bundling.
117. Two respondents called for additional clarity around the concept of "access to historic series on a per-week basis", which they said may not be feasible for regular users of the trading platform (for cost reasons). Here they note the importance of a distinction between users of the trading platform for trading activities and those who use (or buy) the data for further aggregation and value-added services.
118. Another respondent supported disaggregation on a per-crypto-asset basis, however, they objected to the transparency data requirement including all transactions involving a crypto-asset (on a daily or more frequent interval).

**Q36: In the context of large number of CASPs and possible different models of data access, what kind of measures (common messages, common APIs, others) would you consider feasible to ensure effective and efficient access to data?**

119. 13 respondents highlighted the need for harmonized measures to share and access data. Suggestions on concrete measures included APIs (six respondents), S3 buckets (one respondent), and decentralized oracles or blockchain explorer for on-chain data (one respondent).
120. Three respondents supporting harmonization suggested to not set strict rules but general guidelines and allow for some freedom to customize fields and parameters.
121. Furthermore, two respondents specifically mentioned these measures should be defined by ESMA similarly as enabled by the empowerment in Article 26 of MiFIR.
122. Two respondents highlighted that measures in this context should also avoid any misalignment with measures stemming from FIDA.
123. Two respondents argued that the measures should allow for protocols to be recycled and deployed in open source to facilitate the harmonization.
124. One respondent highlighted that measures should allow for backward compatibility, input validation, and encryption. This respondent also highlighted that CASP and NCA staff should be trained to best apply these measures.
125. One respondent, a pan-EU trade association representing a wide range of sell-side market participants mentioned standardized file formats, specifically mentioning the JSON format, would be feasible to ensure effective and efficient access to data.
126. One respondent suggested for these measures to not only take inspiration from the traditional financial sector but also the crypto-asset industry which might offer more suitable solutions which will continue to improve as the industry grows.

127. Four respondents did not suggest any particular model of data access or measures relating to them.
128. Of these, two argued that no measures are required because DLT already makes information transparent, one of which welcomed flexibility on format in RTS but also highlighted RTS appear to be inapplicable to CASPs that only carry out transactions classifiable as crypto-asset transfers between wallets (e.g. fields “buyers” and “sellers” are not suited for this type of transactions). Furthermore, this respondent argued that requirements replicating those of MiFIR would be too burdensome for CASPS and their clientele which are unaccustomed to these types of requirements.
129. One respondent argued to allow for different models to organically develop and notably to avoid burdensome requirements for the production and sharing of data that is not useful to market participants.
130. One respondent did not specifically respond to the question at hand but argued that the record keeping as proposed in the RTS is too burdensome and goes beyond legal basis of MiCA.

**Q37: Do you agree with using the DTI for uniquely identifying the crypto-assets for which the order is placed or the transaction is executed? Do you agree with using DTI for reporting the quantity and price of transactions denominated in crypto-assets?**

131. A large majority of respondents supported the proposal, either outright or with some comments. Seven respondents supported the proposal to use the DTI for both purposes outright.
132. Two respondents supported the use of DTI as a good starting point but that the definition of the token matrix definition would be welcome.
133. Two respondents noted some doubts on the diffusion of market practices around DTIs, highlighted the potential for fragmentation, and recommended monitoring in case other crypto native identifiers emerged. One respondent supported the use of DTIs but suggested supplementing it with additional fields and also considering the FIGI standard.
134. One respondent supported the proposal but also added that the field “Smart Contract Addresses” in Table 3 of the Annex to the RTS on content format and order book records should allow up to 100 characters (rather than 52) to be future-proof.
135. Two respondents supported the efforts to introduce a unique identifier in the DTI but urged ESMA to consider other projects as well, including ones based in Europe and with more transparent governances.
136. One respondent agreed with the use of DTI for both purposes but highlighted that the notion of token was too large under it.
137. One respondent agreed with the proposal while emphasizing the need to ensure that this would not create undue burden and costs on smaller players.

138. Four respondents disagreed with the proposal made.
139. One respondent questioned why the standard chosen in the RTS was being assigned by a firm (underpinning the DTIF) based outside of the EU. The lack of distinction between coins and tokens was also pointed.
140. One respondent argued that DTI should only be included in the White Paper while for transaction reporting the standard on which to rely should be the ISIN/ITIN to avoid creating redundancies.
141. One respondent expressed concerns regarding the speed of assignment of DTIs and advocated for a temporary option.
142. Finally, one respondent supported using a unique identifier but argued against using the DTI as this unique identifier because its adoption is not broad enough and that there are more efficient identifiers that could be used (i.e., token addresses/contracts).

**Q38: Are there relevant technical attributes describing the characteristics of the crypto-asset or of the DLT on which this is traded, other than those retrievable from the DTIF register? Please detail which ones.**

143. Four respondents considered that the technical attributes retrievable through the DTIF register were sufficient to describe the characteristics of the crypto-asset or of the DLT on which it is traded.
144. Additional attributes deemed as relevant by respondents were token definition contract for secondary tokens defined through smart contracts (three respondent), the token standard (two respondents), references to other identifiers (one respondent), tokenomics (one respondent), environmental impact (one respondent), information on a standardized rounding of asset quantities (one respondent), hashing power for Proof of Work Coins (one respondent), and issuers' ID or LEI (one respondent).
145. One respondent suggested keeping the attributes simple to not mislead investors while another respondent suggested a simplification of the display of the information to make it more descriptive accessible to a larger public (i.e., a recognizable name rather than a code for certain fields).
146. One respondent did not respond directly to the question at hand, highlighting crypto-assets' attributes could be identified in other ways than through the DTIF register.

**Q39: Do you agree with using the transaction hash to uniquely identify transactions that are fully or partially executed on-chain in orders and transactions records? Please clarify in your response if this would be applicable for all types of DLT, and also be relevant in cases where hybrid systems are used.**

147. 11 respondents agreed to proceed with ESMA's proposal of using the transaction hash as a unique identifier for fully or partially executed on-chain in orders and transactions records as long as the integrity of the transaction is guaranteed. A couple of respondents,

while not disagreeing with its use, suggested that it might not be in all cases identifying these uniquely since multiple trades can be settled in one transaction.

148. One respondent clarified that transaction hashes could potentially represent a multitude of actual transactions possibly relevant for multiple users, putting in question their usefulness as unique identifiers for these transactions.
149. Respondents generally fully supported ESMA's suggested approach that any additional means of identification would present an unnecessary burden to trading platforms when an on-chain transaction is performed.
150. With regards to situations where hybrid systems are used, several respondents supported the use of the transaction hash as the best means to uniquely identify transactions all while warning of its limitations in these cases.
151. One respondent considered less clear whether hybrid systems would need a more nuanced approach to ensure that transactions are accurately and reliably identified regardless of whether they are executed on-chain, off-chain, or through a combination of both. Another respondent suggested adding a field for "linked transaction" to address this.
152. One respondent disagreed with the use of transaction hashes in favour of a more technology neutral term.

**Q40: Do you agree that a separate field for the recording of "gas fees" should be included for the purpose of identifying the sequencing of orders and events affecting the order?**

153. While a plurality of respondents agreed with the usefulness of providing a field to register "gas fees" for on-chain transactions, many did not believe this to be absolutely necessary or a priority for the purposes of these TS. Some respondents question the ability of determining the sequencing or prioritization of orders thanks to this field due to the way gas fees are structured and combined with other fees.
154. Other respondents did see the usefulness to include them for even further purposes, such as identifying trading patterns such as high-frequency trading or activities of market makers. Some respondents questioned their usefulness for trades involving hybrid systems.
155. One respondent signalled the fact that this term is commonly used to refer to Ethereum fees and suggested to keep the approach technology-neutral, suggesting the use of the name "transaction fees". Another respondent suggested the more general name of "network fees".
156. Some respondents mentioned the fact that other fields in these RTS (i.e., transaction hash, timestamp) could help achieve the same goals without including a field for "gas fees".



157. Other respondents suggested that ESMA should further clarify the specific cases for which it intends to use this information and suggests this field to be made voluntary.

**Q41: Do you agree with the inclusion of the above data elements, specific for on-chain transactions, in both RTS?**

158. The vast majority of respondents supported the inclusion of the suggested data elements for on-chain transactions, with wide support to the inclusion of a specific on-chain trading data table. Some respondents however, signalled that creating a custom standard may impede its applicability to all digital asset technologies.

159. Some respondents made reference to suggestions to other fields previously discussed in this report and which have already been addressed.

160. One respondent asked for clarifications with regards to data privacy issues and asked for reassurance in case the information cannot be retrieved from unhosted wallets.

**Q42: Are some of the proposed data elements technology-specific, and not relevant or applicable to other DLTs?**

161. With a few exceptions who confirmed their universality, albeit with different names. As explained in the previous section almost all respondents identified: gas fees, gas limits and certain as well data size and smart contracts as specific to certain technologies, most commonly Ethereum. Respondents suggested to adapt these requirements to be more flexible to the different technologies, while reminding the different technologies and their similarities and differences when it comes to achieving the objectives those fields were set up to.

162. One respondent suggested that there might be issues when it comes to identifying the fields “Quantity/ Current Total Supply”.

163. One respondent suggested that the use of timestamps could be combined with the use of the hash identifier to better relay the information when it refers to the order of the transaction. As explained in previous sections, they also suggest that the use of DTI should be able to cover this in a more precise manner.

164. Finally, one respondent suggested a small wording amendment to article 2 on the requirements for the conditions to be met for the retention of records while another respondent supported the current proposal for said article.

**Q43: Do you consider it necessary to add a different timing for the provision of identification codes for orders in the case of CASPs operating a platform which uses only on-chain trading?**

165. A majority of respondents agrees that CASPs operating a platform that uses only on chain trading should be allowed to have a different timing for the provision of identification of orders due to the unique characteristics of the blockchain technology and the time it

needs for the processing of the transaction, block creation and confirmation as well as congestion of the networks and settlement timing.

166. One respondent disagreed by stating that the fact that transactions can be given immediate identifiers is proof that orders can do so equally. The respondent notes there are several technological solutions available to ensure this.
167. One respondent supported the differentiation while making certain remarks on the timing of the provision of the information that seem to concern more transaction information rather than only one relating to orders.

**Q44: Please suggest additional data elements that may be included to properly account for on-chain trading.**

168. Several respondents suggested or supported the inclusion of certain additional data fields to properly account for on chain trading specificities.
169. There were some respondents supporting ESMA's inclusion of hash, or combining it with the HMAC or other pointers to identify data stored in off chain databases. Other respondents suggested the inclusion of Method ID to allow for the provision of details on the type of transaction and the function call for ERC20 tokens. However there were again mentions to avoiding technology specific terms (such as Method ID) or "gas fees".
170. To complement the information already included by requiring the hash, one respondent suggested including a field for an identifier that would signal the unique order of outputs inside a transaction hash if there are multiple outputs for multiple users. The suggested identifier, "vout" or "vector output" seems to be one related mostly to Bitcoin.
171. Two respondents suggested including the trade execution dates as a separate field and underlined the importance of being able to timestamp the creation of the block and the execution of the trade.
172. Finally, one respondent explained that the complex trade component ID as applied in the context of trading in crypto assets could pose significant challenges as it already does in the world of derivative trading. They suggested against the implementation of an identifier resembling the transaction record number to avoid the complexities of its implementation for market participants in the context of a much more anonymised market.

**Q45: Do you find the meaning of the defined terms clear enough? Should the scope be adjusted to encompass or exclude some market practices? Provide concrete examples.**

173. Almost every respondent supported the proposed definitions as they stand. One respondent suggested for the general approach to the definitions to have a more technology-neutral stance, a fact that has been reflected throughout this report.
174. Another respondent suggested several terms to be included as further defined terms in the definitions of the text to better cover the rapid nature of evolving practices in the

crypto assets market. A different respondent suggested clarifying the scope of transactions that would fall under the record keeping requirements.

175. Furthermore, one respondent suggested a clarification of the definition of undertaking a transaction that would reduce the proposed scope which is currently based on the executing a transaction definition of RTS22.

**Q46: Are there other aspects that should be defined, for the purposes of this RTS?**

176. Almost every respondent believed no further definitions should be added to the RTS. One respondent asked for the inclusion of general business continuity requirements from the perspective of the CASPs. Another respondent requested to clarify the scope of the recordkeeping requirements as it relates to parties other than the CASP which are involved in the transaction.

**Q47: Do you anticipate practical issues in the implementation of the proposed approach to reception and transmission of orders?**

177. While a majority of respondents consider that there should not be issues with the proposed approach to the reception and transmission of orders, several respondents noted potential issues when it comes to transmission of orders from 3rd country CASPs or trading platforms.
178. Some respondents signalled that given the fact that 3<sup>rd</sup> country entities would not fall under the scope of MiCA there could be issues both of lack of information provided as well as issues in terms of data standards and formats.
179. Additionally, issues related to technology-related data protection safeties could play a role as part of the reason behind missing information.
180. The transmission and reception of orders from third countries had already been identified in ESMA's Consultation Paper as a major issue when it comes to ensuring the retrieval of the data by CASPs.
181. The approach of allowing CASPs to demonstrate a best effort scenario whenever information from these kinds of orders is missing has been raised by certain respondents as having certain benefits from a supervisory point of view. There is a risk, however that this would lead to lower effort from CASPs to retrieve information from third country parties.

**Q48: What transaction information can be retrieved in cases where a CASP execute the order on a third country platform/entity?**

182. In order to reflect the fact that CASPs will depend on third parties not subject to MiCA to retrieve certain information, ESMA proposes to introduce a clarification to reflect that CASPs should record-keep this information stemming from the routing of orders from third country entities whenever this information is retrievable.

183. Certain respondents suggest including a flag signalling the country of origin and destination when applicable while others believe that the buyer seller flag might not be available when dealing with decentralised exchanges. Furthermore, support to the inclusion of all other fields included for EEA undertaken transactions, especially including the use of LEI was expressed by another respondent.

**Q49: Do you anticipate problems in retrieving information about the buyer/seller to the transaction?**

184. As covered previously in the responses to other questions in this report, the majority of respondents agreed that there are likely to be several issues when retrieving information not only concerning the buyer/seller of the transaction, with a special emphasis on transactions involving third countries.

185. Respondents noted that both when it comes to centralized and decentralised exchanges, in many situations, entities or individuals not subject to MiCA would generate a void of information, including but not limited to their lack of obligation to have an LEI.

186. In that line, some respondents noted that mandating CASPs not to allow trading to parties that do not have an LEI would cause severe market disruption.

187. Furthermore, several respondents agreed that due to due diligence and know your customer requirements being different across jurisdictions, CASPs will have issues retrieving some of the information.

188. A few respondents signal the importance of ensuring privacy and the fact that this can both cause lack of information when it comes to transactions involving third countries, but that it should also be ensured as much as possible by avoiding the recording of plain information whenever this can be substituted by anonymised means.

**Q50: Do you anticipate practical issues in the implementation of the methods for client identification that are used under MiFIR?**

189. More than half of the respondents did not see any practical issues, there is a clear need to implement methods for client identification. They supported the approach that parties involved in transactions eligible for an LEI should be identified as such. If a party is a natural person, national identifiers should be used as per the approach in other financial legislation (MiFIR), since Firm-specific codes may not provide a unified method for identifying natural persons, potentially hindering uniqueness and market activity regulation.

190. However, some respondents anticipate practical issues, such as high admin burden for customers and CASPs.

191. One respondent considers it prudent that ESMA includes an exemption from the requirement for authors of white papers to obtain an LEI, where they are not eligible for an LEI or where one cannot be obtained despite reasonable commercial efforts.

192. Two other respondents believe that the approach may hinder DEXs and other decentralized applications, initially designed to preserve wallet addresses. Adding that future exemptions could be based on low value transaction thresholds. However, as mentioned in the PwC study a solution would be that “To ensure compliance regarding the personally identifiable data obtained during the KYC process, such data could be stored off-chain along with a unique identifier for every market participant that has successfully undergone the KYC process at a DLT market infrastructure”. Another idea is to have the venue communicate encrypted or hashed versions of the data on the Client ID linked to a particular wallet address with the regulator.
193. Another respondent thinks that the proposed national identifiers are ineffective due to discrepancies between national set-ups. Using the full name of the customer as identifier is deemed sufficient here for record keeping (refer to “The travel rule”/ Transfer of Funds Regulation). However, given that the current regulations regarding transfer of fund/travel rule will be extended to the scope of crypto assets, additional information such as the current LEI of the originator, or any other available equivalent official identifier would be required.

**Q51: Do you anticipate practical issues in the implementation of the short selling flag?**

194. Half of the respondents do not think there are any practical issues. Those who are anticipating practical problems, however, appear to be the result of definitional problems; the responses ask for a clarification of the short selling concept. If a short selling flag results from trading on derivatives, it will not affect services covered by MiCA. But there is some confusion because the ability to lend a cryptocurrency asset makes it possible to execute a short sale position. If ESMA refers crypto-asset lending or if different cases, it is requiring additional consideration.
195. Furthermore, flagging for short selling requires constant monitoring, covering all the current techniques might be complex. It can be difficult because of the complexity of short selling for CASPs to appropriately record and report such activities, thus they must modify their systems and procedures.

**Q52: Do you consider that some of the proposed data elements are not applicable/relevant to trading in crypto-assets?**

196. Most respondents agreed with the relevance of the proposed data elements while supporting a uniform approach to data formats. However, a couple of respondents believed that some of the proposed data elements might make the regime too detailed including data fields related to investor protection that might not be relevant for crypto assets markets.
197. Some respondents made reference of their support to the conclusions of the study on DLT Pilot regarding the applicability of certain of the fields to DLT technology.

**Q53: Do you consider that additional data elements for CAPS operating a trading platform are needed to allow NCAs to properly discharge their supervisory duties?**

198. All but one respondent suggested no additional data elements are needed to adequately allow NCAs to exercise their supervisory duties. One respondent reminded the fact that a Refit of the text could allow further fields to be added in case of future need.
199. One respondent suggested that additional data elements might be required without specifying any data fields that could be included.

**Q54: Do you believe that a specific definition of routed orders should be provided as it applies to orders that are routed by the trading platform for crypto-assets to other venues? Should this definition include CASPs operating a platform which uses only on-chain trading?**

200. All but two respondents agreed with ESMA's approach and signalled the importance of having a clear and specific definition of the routing of orders with a preference to orders happening on only on-chain venues being included in this definition.
201. One respondent considered the inclusion of the fields concerning the routing of orders in the annex should be enough to allow this information to be available to supervisors.

**Q55: Do you believe that fill-or kill strategies as referenced in MiFID II apply to trading in platforms for crypto-assets? Do they apply to partially filled orders?**

202. Almost all respondents agreed that fill-or-kill strategies are not only relevant but also very common when trading in crypto assets and therefore expressed their support for their inclusion in these RTS.
203. On their compatibility with partially filled orders, several respondents clarified the fact that these strategies are not compatible and should therefore not be recorded as such when accounting for recordkeeping data.
204. One respondent stated that these strategies might be conflicting with other strategies currently practised by CASPs, without suggesting any changes to reflect that statement.

**Q56: Do you agree with using messages based on the ISO 20022 methodology for sharing information with competent authorities?**

205. Most respondents clearly supported the use of messages based on the ISO 20022 methodology for sharing information with competent authorities.
206. One respondent was supportive of the use of ISO 20022 but did not recommend its implementation for these purposes before ESMA allows sufficient time for testing the standard's interoperability with Blockchain systems and their interactions with third-parties (i.e., NCAs in the context of MiCA).
207. One respondent signalled that they had not received confirmation from their members regarding their implementation of this standard when sharing information with competent authorities and would therefore urge ESMA to keep a flexible approach that would not pre-empt the standard that the industry might choose for these purposes.



**Q57: Do you agree with the criteria proposed for identifying a relevant machine-readable format for the MiCA white paper and consequently with the proposal to mandate iXBRL as the machine-readable format for MiCA white papers, subject to the outcome of the study referred to in paragraph 239?**

208. 16 respondents provided input to this question. Of these, 12 agreed with ESMA's proposal to introduce iXBRL as the format of the white paper or agreed with the proposal to rely on the outcome of an independent study.
209. One respondent did not express a strong preference but suggested that data extractability could be sufficient (rather than machine-readability) in light of the objective co-legislators tried to pursue with the white papers. ESMA reminds stakeholders that its legal mandate is to specify a machine-readable format, and that therefore it cannot legally mandate a data extractable format instead.
210. Two respondents argued that it would be preferable to leave the choice of the machine-readable format to the preparers; one further argued that human-readability is not a requirement stemming from Level 1. ESMA acknowledges that human readability is not a Level 1 requirement but only a "nice-to-have"; however ESMA's mandate is to "specify" a format, therefore leaving free choice to preparers would not be compliant with its legal mandate.
211. One responded highlighted that iXBRL is typically used for financial statements rather than for free text disclosures. ESMA wishes to highlight that sustainability reporting pursuant to the CSRD is constituted largely of textual information and is expected to be in iXBRL format, which therefore is not only adopted for financial statements-like disclosures.
212. This same respondent argued that ESMA should develop an online submission form, rather than leaving to individual businesses the burden to obtain a license to create an iXBRL report and that the estimated costs for regulators are excessively high. In light of the support received for the Excel converter tool published together with the Consultation Package (see responses to Question 65) ESMA deems it sufficient at this stage to aim to provide to preparers a simple conversion tool rather than an online submission form, whose development costs are much higher and the deadlines much longer than a simpler tool. ESMA also highlight that the Consultation Paper did not include estimated costs for regulators in the context of MiCA and that the range of costs indicated in the context of the ESEF project are not expected to be representative of the costs for receiving and validating MiCA white papers. The independent study commissioned to Gartner provides additional details about the costs expected for all stakeholders.
213. One respondent highlighted that it is essential that the whitepapers can contain graphics/images to complement technical explanation. ESMA notes that iXBRL is the only machine-readable format which has been identified so far which allows for the smooth inclusion of graphics and images. Finally, one respondent argued that the concept of white paper is no longer very relevant, as most crypto asset projects publish their information on Gitbooks and the information contained therein needs to be



constantly updated (which they noted may not be compliant with iXBRL). ESMA notes that this ITS responds to a legal mandate contained in Level 1 and that it goes beyond ESMA's mandate to assess the relevance of the concept white papers.

**Q58: If yes, do you agree that the white paper should be required to be a stand-alone document with a closed taxonomy (i.e., without extensions nor complex filing rules)?**

214. Seven respondents provided their feedback on this question. The vast majority of them agreed with the proposal to require that the white paper to be a stand-alone document with a closed taxonomy. One respondent encouraged ESMA to provide minimal filing rules to define, for example, the acceptable formats for images, the CSS styles and so forth. ESMA will indeed consider providing filing rules, as was done for other machine-readable formats prescribed in the past.
215. Two respondents highlighted the need to keep flexibility to account for future technological or market development, which ESMA intends to do compatibly with the requirements included in L1.
216. One respondent stressed that it would be desirable that the white paper format was compatible with the KID regulation. ESMA highlights that closer compatibility is expected to be achieved with the coming into force of the ESAP Regulation, but that the scope of its proposed rules are limited by the mandates contained in level 1 legislation.
217. Finally one member urged ESMA to accept additional information to be provided within the white papers. As described in the Consultation Paper, however, the MiCA Regulation does not foresee the possibility that information other than that explicitly required by Level 1 may be added in the white paper. Additional information can however be included in marketing material.

**Q59: If not, please elaborate your answer and propose alternative solutions that would best meet the criteria identified in section 7.3.**

218. Seven respondents provided input to this question.
219. One respondent suggested that several PDFs make data extraction process possible. ESMA reminds stakeholders however that the chosen format should be machine-readable and not data-extractable only, and that none of the existing types of PDFs meets the definition of "a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure", which is provided in L1 legislation and in particular in the ESAP Regulation (which is relevant since the MiCA white papers will be collected in ESAP starting from 2030). For that reason, it is important that the definition of machine-readability adopted in the context of MiCA is the same as that prescribed in the context of ESAP. This is also recommended by the Commission in the context of the Strategy on supervisory data to ensure consistency and harmonisation of reporting requirements.

220. Another respondent suggested that ESMA should develop an online form on its website, through which individual firms can submit the information required for the white papers. Please see paragraph 0 for a response to this point.
221. Finally, one respondent tentatively suggested a hybrid model of a token card coupled with an attachment that describes any specific addenda for the token in question, another suggested a link to the relevant Gitbook. ESMA deems that these proposals would not be compliant with the mandate in MiCA Level 1.

**Q60: Are you currently preparing white paper documents in a different machine-readable format? If yes, which one?**

222. Seven respondents provided input to this question.
223. No one said another machine-readable format is currently being used.
224. One respondent noted that the majority of whitepapers issued in the past were formatted as machine-readable PDFs. While this approach has been prevalent, they also recognised the necessity for standardisation and the benefits stemming from the coherent provision of information as mandated by the MiCA regulation.

**Q61: How different is the white paper mandated by MiCA and further specified in this Consultation Paper from any white paper which you have drawn up or analysed prior to MiCA? Do you think that any additional information that used to be included in white papers prior to MiCA but that is no longer allowed under the relevant provisions of MiCA for the white paper will continue to be made available to investors as marketing communication?**

225. 11 respondents provided input to this question. Several respondents highlighted that the main novelty brought by MiCA is the high level of standardisation, which is expected to prevent bespoke information (which can be provided only in marketing material). One respondent noted that information mandated under the new regime is more granular, and argued in favour of additional exceptions as it is the case for prospectuses. ESMA notes that it is beyond its mandate to provide exceptions to Level 1 requirements.
226. One respondent noted that usually before MiCA, white papers contained a section on Tokenomics. Another member noted that the format was in most cases PDF. Another respondent noted that the focus of the MiCA white paper is mainly financial, while the previous white paper had a larger focus on technological features. Furthermore, sustainability-related information did not use to be disclosed in white papers.

**Q62: Do you agree with ESMA's estimate of the cost of preparing a white paper in iXBRL format? If not, where would you put the estimate of a preparing a white paper in iXBRL format (not considering costs of information sourcing which should be considered as base scenario)?**

227. 12 respondents provided input to this question. The large majority agreed with ESMA's estimate of the cost of preparing a white paper in iXBRL. One respondent estimated that

a white paper on the basis of the draft requirements would cost 2500 euro. However, ESMA directly followed-up with this respondent to understand how this estimate was reached and the respondent clarified that this cost does not regard the format specifically but rather the cost of drawing up a white paper on the basis of the existing MiCA requirements as specified in Level 1.

228. Two respondents expressed no view on costs for preparers, but one argued that a cost of up to 33k for regulators (estimated on the basis of the experience of ESEF) was not acceptable for the expected level of benefit for users. ESMA would like to highlight that, as discussed in the Consultation Paper, the highest estimates of cost derive from studies on the basis of much more complex reporting requirements for financial reporting, and therefore that the estimated cost of iXBRL for regulators is expected to be much lower than that faced to receive and validate financial reports.
229. Finally, one respondent argued that the cost estimates must reflect the cost of including graphics. ESMA notes that iXBRL is the only machine-readable format that allows graphics to be embedded in the white paper. The cost of embedding graphics however should not be considered as part of the baseline cost since there are no requirements in MiCA to provide images / graphs which are therefore not mandatory but may be provided on a voluntary basis.

**Q63: Do you agree with the proposed template for presenting the information as indicated in the Annex to this CP? We welcome your comments on the proposed fields and values/descriptions to be included in the fields - please provide specific references to the fields which you are commenting in your response and pay specific attention to the areas where additional explanatory description of the information is provided.**

230. 11 respondents provided input to this question. Most deemed the proposed template to be largely effective. Some respondents provided drafting suggestions.
231. One respondent noted that there might be practical difficulties to fill in information on the issuer for token issuers which are DAO (“Decentralised Autonomous Organizations”) because token issuers may not be structured like traditional companies. Similarly this respondent asked for guidance for the field “Members of the management body” as in some cases issuers do not have a traditional formal management structure (for example in the case of foundations, or projects where after the launch there is no longer a “core team”).
232. This respondent also encouraged ESMA to clarify that the section about “plan for the token” is not contractually binding, and that the field “resource allocation” should be better defined to clarify what type of resources (financial, human etc.). This respondent also noted that in case of token sale including a price discovery mechanism it would be challenging to provide information about the offer. ESMA took note of these suggestions and has provided some guidance in the ITSs whenever possible and/or relevant within the confines of the Level 1 mandate. Additional guidance may be provided as L3 guidance if necessary.

233. A respondent indicated that telephone numbers should not be mandatory fields. Another noted that LEI nor national identifiers should be required from smaller issuers. ESMA notes that it goes beyond its mandate to remove certain fields from the template or from the obligations of certain issuers.
234. A respondent argued that ESMA did not take a proportional approach in its proposal and that MiCA recital 24 was not sufficiently considered. ESMA would like to highlight in this regard that Level 2 RTS/ITS do not affect the requirements / provisions of MiCA Level 1, and therefore as indicated by recital 24 and article 2 paragraph 3, the provision of MiCA and consequently of ESMA's ITS/RTS do not apply to crypto-assets that are unique and non-fungible with other crypto-assets. It is beyond ESMA's mandate to provide other exceptions.
235. One respondent suggested that not all fields should be mandatory. ESMA notes that Article 6 of MiCA unambiguously requires that a crypto-asset white paper should contain all the information included in Article 6 paragraph 1 and further specified in Annex I. Therefore it is beyond ESMA's mandate to exempt preparers from providing certain information.
236. One respondent suggested that certain additional fields should be added. ESMA reminds stakeholders that the list of fields is pre-determined by the MiCA Regulation and that it is beyond its mandate to add new fields. One respondent suggested to specify which language (if any) is perceived to be the prevailing language in case of a conflict between various different languages of the white paper. ESMA notes that the field language is not relevant in the white paper but will be part of the information submitted as metadata as specified by the [Delegated Regulation xxx/xxx RTS on data for classification of the white papers].
237. Another respondent provided some drafting suggestions on Table 4, field E3, which were duly taken into consideration.
238. One respondent argued that ESMA should allow for additional fields such as roadmap, unique value proposition, tokenomics etc.. ESMA highlights that this goes beyond its mandate as it contradicts article 6 paragraph 1 of MiCA. This respondent also highlighted the need for ESMA to allow the inclusion of graphical designs, which ESMA would like to highlight are indeed not disallowed.
239. Finally, one respondent stressed that the reliance on free text could lead to inconsistency in the information reported and encouraged ESMA to provide more detailed guidelines or examples for each field to ensure clarity and uniformity in reporting. ESMA strove to provide as much guidance as possible in the draft ITS but notes that additional guidance may be provided as L3 (for example, as a Q&A), also in light of the best practices that will emerge in the first years of implementation of the new requirements.

**Q64: Are there additional data elements in the table of fields that would benefit from further explanatory descriptions to ensure that the information provided by a given issuer/offeror is understandable and comparable to the information provided by other**

**issuer/offeror of the same type of crypto-asset? If yes, please elaborate and provide suggestions.**

240. 10 respondents provided views on this question. One respondent suggested to delete the field “national ID identifier” as it is not used. One respondent encouraged ESMA to provide additional guidance on certain fields to specify whether the cost and expenses referred to should relate to costs borne by the investor, or the offeror, or the person seeking admission to trading of the crypto-asset.
241. Another respondent suggested to use the iXBRL concept of type `xbri:stringItemType` for the “predefined alphanumerical text” and for all Yes/No values. ESMA notes that the technical details of XBRL item types are not included in the draft ITS but will be specified in the taxonomy files.
242. One respondent noted that liability for the disclosed information may not be clear where the preparer is not the issuer but the offeror. This respondent believes that the liability always sits with the original preparer and encouraged ESMA to provide clarity on this type of issues via its Q&As. This respondent also noted that some information requested is not applicable across the spectrum of crypto assets, i.e. many issuer do not have a legal personality, as they may maintain anonymous presence for security or privacy reasons, and encouraged ESMA to provide further clarify on certain fields. ESMA may consider to provide such clarifications in future guidelines/Q&As.
243. Finally one respondent encouraged ESMA to provide more detailed and structured guidance/ templates on the sustainability indicators in part J. ESMA notes that this is provided for in the *RTS on content, methodologies and presentation of sustainability indicators on adverse impacts on the climate and the environment* covered in Section 2.

**Q65: Would you deem it useful for ESMA to provide an editable template to support preparers with the compliance of the format requirements proposed in the draft ITSs?**

244. All 17 respondents would deem it useful for ESMA to provide an editable template to support preparers with the compliance of the format requirements. One respondent highlighted that it would be preferable to choose an open-source solution.

**Q66: Are there any other data elements that you would consider relevant to ensure that investors can properly compare different crypto-asset white papers and NCA can perform their classifications on the basis of harmonised information?**

245. Three respondents estimated that the data elements to be reported in white papers were sufficient.
246. Additional attributes deemed as relevant by respondents were provisions fostering comparability for investors<sup>56</sup> (three respondents), the governance structure and mechanisms (two respondents), last update date and version number (one respondent),

---

<sup>56</sup> These referred to either historical data (such as historical data on token value) or enabling comparison at a given time (such as against yardsticks for sustainability indicators).

auditing firm's name (two respondent), tokenomics<sup>57</sup> (two respondents), the exchange ticker, in addition to the MIC, as the former is more likely be assigned than the MIC (one respondent), roadmap (one respondents), unique value proposition (one respondent), detailed consensus mechanism description (one respondent), risk management practices (one respondent), compliance status (one respondent), and developer and management team backgrounds (one respondent).

247. Furthermore, three respondents commented on the need to allow some flexibility and avoid limitations. Two recommended to do so by ensuring it is possible to make references beyond White Paper and one respondent by recommending an iterative model to ensure that data elements can be added over time.

248. Finally, one respondent asked that it be specified that all data elements required in White Papers would only be so where NCAs have full enforcement capacities.

**Q67: Do you agree with ESMA's conclusion that an issuer, an offeror or a person seeking admission to trading of crypto-assets should always be eligible for an LEI? If not, please provide a description of the specific cases**

249. 13 respondents provided views to this question. There was very broad support for the requirement to obtain an LEI for eligible entities.

250. A specific case of non-eligibility was mentioned: issuers are not identifiable in the case of "decentralized autonomous organisations". Indeed, there is a need to investigate whether the concept of "issuer" can apply to this specific case. ESMA will engage with the respondents that raised this question to assess alternative means of identification for this specific case.

**Q68: Do you agree with the proposed metadata elements, also considering the mandatory metadata expected to be mandated in the context of ESAP?**

251. 7 respondents provided views to this question. All supported ESMA's proposal with regards to metadata. One respondent noted that some consideration should be given to categorisation of projects with no identified issuers or LEI and to ENS domains and Twitter domains.

252. One respondent disagreed with the use of the LEI, which it deemed too burdensome for small issuers. Please refer to question 67 for a specific response on LEIs.

**Q69. Do you have any feedback in particular with regards to the metadata on the "industry sector of the economic activities" and its relevance for the ESAP search function?**

---

<sup>57</sup> Defined to include many different aspects of crypto assets ranging from economic models to detailed consensus mechanism descriptions



253. Two respondents provided views on this question. One believed that the categorisation should be adapted to the digital assets sector and be more granular - e.g. yield farming, gaming, stablecoins, peer-to-peer, payments.

254. Another respondent agreed that the metadata requirements for crypto-asset issuers and CASPs should be aligned with existing classification of economic activities.

**Q70: Do you agree with the listed definitions? Would you consider useful to clarify any other term used in the ITS?**

255. 14 respondents provided their feedback to this question. Respondents generally agree with the listed definitions. Some asked for additional clarifications, as follows.

- i. On "media which are reasonably relied upon by the public", it was noted this is a key and quite vague term;
- ii. On 'durable medium', web-based platforms' and 'social media', clarifications were asked on how they specifically apply in the context of MiCA; for 'web-based platform', one respondent suggested using the definition from Article 3 (i) of the Digital Services Act;
- iii. On "significant effect on the prices of crypto-assets" it was asked to clarify when inside information should be disseminated;
- iv. It was suggested to use a more nuanced approach on the 'inside information' term, as it is quite broad, and it may be compatible with stablecoins only;
- v. It was asked to specify whether "trading platform for crypto-assets" means a platform operated by a centralized CASP;
- vi. It was also asked to clarify the meaning of what is information that "directly concerns them [the issuers]". It was also noted that Level 3 guidance may be required on this wording;
- vii. There was also a general request on explanations and examples on the terms and concepts specific to CAs and blockchain.

256. Only one respondent was less supportive of the list of definitions, and pointed out information could be needed on whether a trading venue / marketplace intends to list or delist a crypto asset, or whether someone intends to buy or sell a larger (price-influencing) package.

**Question 71: Do you agree with the proposed requirements for publication on the website of the issuer, offeror or person seeking admission to trading? Would you consider necessary any additional requirements regarding the publication on the website?**



257. The majority of respondents agreed with the proposed option for publication on the website of the issuer. A few respondents called for additional specifications beyond what was presented in the draft ITS, including: a format or template for the publication of inside information on the website (e.g. standardised sections or headings to ensure consistency, enhance readability and accessibility for investors and the public); and features to enhance the accessibility of the publications as archiving and historical access, a search functionality, interactive elements (like FAQs or chat support) and features ensuring accessibility for persons with disabilities.
258. One respondent stated that the use of 'opt-in alerts' may favour investors who make use of trading bots or high-frequency trading techniques, as they rely on alerts to access to instant information as part of their strategy. As a result, opt-in alerts could also possibly increase market volatility.
259. Few respondents shared the concern that issuers might not have a website on which to publish the inside information, advocating for more flexibility for publication of the inside information, (for example by allowing the use of an RNS).

**Question 72: In your view, is there any obstacle for the website of the relevant parties to allow for specific alerts?**

260. The majority of respondents did not see any obstacle for the website of the relevant parties to allow for specific alerts.
261. Two respondents highlighted that data protection regulations should be taken into account if they might prevent the diffusion of such alerts and that alerts should be designed as "opt in" to avoid noise for end users. A minority of respondents stated they are not in favour of such alerts as they may favour investors who make use of trading bots or high-frequency trading techniques (possible volatility implications, see answer to Q71) and that some users might not be reachable with alerts.
262. Two respondents noted that some websites or browsers might not support alerts, hence they suggest using social media channels or web based platforms to publish info and updates.
263. One respondent reiterated the suggestion to allow more flexibility for publication of the inside information, as an example using an RNS (as per Q71).
264. One respondent did not provide an answer.

**Question 73: In your view, what are the media most relied upon by the public to collect information on crypto-assets? In case you are an issuer, offeror or person seeking admission to trading, please specify/add which media you would normally use to communicate with investors and the reasons supporting your choice.**

265. 14 Respondents provided examples of the types of media that are prevalent in the information ecosystem of the crypto-asset market, including specific named examples of

the tools and/or media outlets they typically use to stay up to date on developments or share marketing and investor-relevant information.

266. Almost all respondents said social media is a common (near ubiquitous) tool that issuers should consider when sharing information related to their crypto-asset offerings with the public. One respondent said many crypto investors have come to expect information to be shared on social media platforms, including for project updates, announcements, and other important product developments. But respondents were mixed about the inclusion of social media in the draft ITS because of concerns about the veracity of information available on social media and the threat of misinformation from fake or unverified accounts.
267. To combat these risks on social media, two respondents noted that the IOSCO standards on digitalisation of retail marketing and distribution may serve as a guide for how issuers (and CASPs) should approach social media, especially with regards to validation of posted information. There was also a recommendation (mirroring the approach in the draft ITS) to have disclosures disseminated through *any* type of media by issuers and offerors to link back to the website of the issuer.
268. Examples of traditional media used by crypto market participants included crypto-specific trade journals (including a list of the top 11 websites by traffic according to the data provider) and outlets that syndicate the financial newswires. Another option was major national publications that now include crypto-asset news in their broader financial market coverage.
269. Several respondents identified crypto market data aggregators and price-tracking websites as two of the most commonly used platforms for disseminating information to investors. One respondent noted that they do not see widespread use by retail investors of professional or subscription-based platforms (for financial advice or real-time data).
270. One respondent said dissemination of any 'price sensitive' information should take place via systems for the dissemination of regulated information ('SDIRs'), leaving only the obligation for the issuer to publish the inside information on their website.
271. One respondent noted that where there was a possibility of opt-in alerts, these were often available through an 'in-app' messaging system whereby issuers can tailor their updates directly for followers of their crypto-asset.

**Question 74: Should a social media or a web-based platform be media reasonably relied upon by the public, what are the risks that you see when using them to achieve dissemination of inside information in relation to crypto assets? Should the dissemination rather take place through traditional media channel?**

272. Of the 14 responses, there were mixed views about the inclusion of social media and other web-based platforms as dissemination channels for inside information.
273. Similar to responses in Q73, several respondents expressed concerns about verifying whether the information published via these channels comes from official sources and

the potential for abuse which could exacerbate market volatility. Another concern raised was the closed nature of certain social platforms such as Telegram, Discord, and Signal which may have barriers to entry in the form of access requirements (e.g., passwords) for a specific channel, group, or server.

274. In general, respondents reasoned that the inclusion of these other two optional elements (in addition to traditional media) would allow issuers and offerors to properly meet the standard of ‘media reasonably relied upon by the public’, with one respondent calling a ‘one-size-fits-all’ approach ‘unsuitable’ to the purpose of the requirement. Forms of media that serve to aggregate information are considered useful insofar as they meet the non-discriminatory and free access standards in the draft ITS.
275. Several respondents questioned whether issuers and offerors would be able to comply with the dissemination requirements in Art. 3(5) of the draft ITS (i.e., assurance of completeness, integrity, and confidentiality of the information maintained during transmission).
276. Another respondent suggested issuers and offerors could rely on a set of standards (developed by ESMA) that would allow them to confirm whether the platform or media in question has sufficiently developed moderation and curation systems in place to ensure the accuracy and reliability of the information disseminated.
277. Several respondents supported the inclusion of traditional media (such as stock market newswires) as a means of dissemination because of the credibility of such platforms, which tend to have stronger editorial standards around what can be published. In fact, one respondent argued that mandating dissemination through at least traditional media (mandatory) would be ideal and perhaps preferable to the multichannel approach described in the ITS because this would limit unfair information advantages for those investors who are ‘in the know’ about which social media platforms / channels to follow for the latest breaking news.
278. By contrast, one respondent (breaking from the consensus view of its trade association) said traditional media is obsolete for reaching crypto investors and therefore would not meet the standard of ‘media reasonably relied upon by the public’.

**Question 75: Please comment on the proposed means for dissemination of inside information. Motivate your answer by indicating why the means are or are not valuable tools for dissemination purposes.**

279. Overall, 14 respondents commented on the means for dissemination proposed in the draft ITS with most calling them valuable. Several respondents (4) expressly noted that communication channels for crypto may need to be different from those used for traditional instruments, especially considering these products attract young and tech-savvy investors. Only one respondent was expressly against the use of social media.
280. One respondent argued that to make the ESMA approach work, there should be a flexible understanding of the principle of “the means relied upon by the public” to allow for issuers and offerors to judge this for themselves. To ensure accuracy of information published

through the dissemination requirement, one respondent again emphasised the usefulness of issuers or offerors including a link to the original publication on their websites.

281. Taking into consideration each of the means of dissemination proposed in the draft ITS, respondents noted the following:

- i. According to two respondents, social media is a means of dissemination most likely used among crypto investors and permitting the fastest sharing of information.
- ii. Half of respondents (7) raised concerns about their reliability and consequent misinformation risk of these social media. Such respondents however do not oppose to their use, rather, they called for requirements to ensure accuracy of information published and the importance of non-discriminatory and free access.

282. One respondent suggested social media and web-based platform to be optional. He noted issuer may not have control over information published on platforms.

283. Only one respondent opposed the inclusion of social media as a means of dissemination, reasoning that these platforms may exclude some investors from the access to information or mix marketing materials with disclosures. The same respondent cited the bureaucratic burden of requiring issuers or offerors to allow push notifications (opt-in alerts). Finally, this respondent called for alignment between the means used under MiCA and MAR because some market participants would be subject to both regulations.

284. Two respondents said websites of trading platforms for crypto-assets should qualify as reliable means of dissemination considering they will be regulated entities.

285. On traditional media, several respondents said it is arguably the most reliable dissemination method given journalistic standards and the in-built fact-checking process, however, the trade-off is slower dissemination compared to the next most relevant alternative: social media. Another respondent noted that traditional media typically has a limited reach compared to social or other digitally-native media.

286. Other suggestions from respondents included:

- i) ESMA conduct research to understand which platforms are empirically the most used means of dissemination and base the proposal on the outcome of the findings
- ii) The development of a central EU web site for regulatory disclosures

**Question 76: Would you add any means of communications for the persons subject to the disclosure obligation to consider when disseminating inside information? Please motivate your answer.**

287. Of the 11 respondents, four indicated no additional means are necessary while three did not express a view. The remaining respondents suggested other means, including:

- i) E-mail newsletters and direct notification via apps. Two respondents said these channels would ensure a fast, direct and prompt communication with investors; and
- ii) Dedicated investor communication platforms for sharing sensitive inside information.

288. A further recommendation was to implement some already existing measures to prevent insider information issues in traditional markets by, for example, requiring issuers or offerors to apply the need-to-know principle or develop an internal “restricted list” for insiders.

**Question 77: Do you agree with the technical means for delaying the public disclosure of inside information as described?**

289. 14 respondents provided their feedback to this question. The respondents agreed with the technical means proposed.

290. One respondent suggested to specify in Article 4 (i) that the explanation of how all the applicable conditions for the delay is to be presented only upon request of the competent authority, where the authority has provided so pursuant to Article 88(3) of MICA.

291. One respondent recalled their answer to Q70, stating that the diversity in types of crypto-assets and the high retail participation in the crypto-assets market may require a more nuanced approach to ‘inside information’.

## 8.4 Annex IV: Draft RTS pursuant to Articles 6(12), 19(11), 51(15) & 66(6) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

**supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts**

**(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<sup>58</sup>, and in particular Articles 6(12), fourth subparagraph, Article 19(11), fourth subparagraph, Article 51(15), fourth subparagraph and Article 66(6), fourth subparagraph thereof,

Whereas:

- (1) Transactions relating to crypto-assets, including but not limited to their issuance, are validated and recorded via consensus mechanisms, namely the rules and procedures to reach an agreement on the validation of a transaction among distributed ledger technology (DLT) network nodes, which are also responsible for holding records of all transactions on a distributed ledger. The achievement of consensus, which among other things requires the use of materials and computing power, comes with climate and other environment-related impacts, which differ across distributed ledger technologies (DLT) depending on their specific features.

---

<sup>58</sup> OJ L 150, 9.6.2023, p. 40.

- (2) The adequate identification and disclosure of the climate and other environment-related adverse impacts linked to the use of consensus mechanisms to issue crypto-assets, is therefore key to the decision-making of those investing in crypto-assets.
- (3) It is important that investors receive accurate, fair, clear, not misleading, simple, concise and comparable information on the impacts of the technologies underpinning issuance of crypto-assets on the climate and the environment. At the same time, given the distributed nature of the technology at hand, it may be difficult to obtain and disclose accurate and reliable information in this regard.
- (4) Persons drawing up the crypto-asset white paper relating to a crypto-asset, including crypto-asset services providers operating a trading platform where relevant in line with Article 5(2) of Regulation (EU) 2023/1114, should be primarily responsible for producing disclosures and should ensure that the format of these disclosures is consistent with the rest of the requirements for crypto-asset white papers. To ensure proportionality in complying with this regulation, persons drawing up a white paper should be allowed to reuse all the information on disclosures on the consensus mechanism that are relevant also to the crypto-asset to which the white paper refers to, where such information has already been published in the context of another white paper, while remaining exclusively responsible for the content of the white paper.
- (5) In turn, crypto-asset service providers should publish these disclosures in a way that facilitates their clients' access to the information as well as the comparisons between the disclosures relating to individual crypto-assets, no matter whether the information has already been made available in a crypto-asset white paper. In the latter case, the crypto-asset service provider is responsible for the generation of the required information.
- (6) Disclosures in the white papers and on the websites of crypto-asset service providers should be reviewed on a regular basis and updated accordingly. The review should ensure coherence across all disclosures in relation to the same crypto-asset. The use of independent third parties to verify disclosures should be disclosed.
- (7) The assessment of the impact of the consensus mechanism used to issue each crypto-asset on the climate and other environment-related impacts requires taking into consideration both the validation of each transaction in the relevant crypto-asset, taking into account the DLT network nodes actively involved in the validation, and the maintenance of the integrity of a distributed ledger of transactions by all DLT network nodes.
- (8) In order to provide appropriate context and ensure investor awareness, mandatory disclosures on the adverse impacts on climate and other environment-related adverse impacts should include a section with general information on the crypto-asset and features of the consensus mechanisms, a mandatory key indicator on energy consumption, and, where relevant, supplementary key indicators on energy and greenhouse gases (GHG) emissions, and a section on the sources and methodologies used to calculate these key indicators.



- (9) To incentivise the use of more climate and environmentally friendly consensus mechanisms and to prevent greenwashing practices, it is crucial to develop an approach relying to the extent possible on quantitative metrics. Quantitative metrics should display gross energy consumption and emissions, without reflecting potential off-setting mechanisms. Considering the considerable role of electricity in the operation of DLT networks, electricity consumption should, in order to facilitate disclosures, be considered a suitable proxy for energy consumption.
- (10) Key indicators should be used to articulate the impacts on climate and other environment-related impacts of the consensus mechanisms in a way that is easy to understand. The key mandatory indicator considered to be the most conducive to investor awareness on the impact of consensus mechanisms is defined as the yearly energy consumption. For crypto-assets with higher levels of yearly energy consumption, supplementary key indicators are defined as the yearly ratio of consumption of renewable energy, the average energy consumption expressed per transaction, the GHG emissions production expressed per transaction and the yearly GHG emissions linked to the use of direct and indirect energy sources.
- (11) In order to ensure a proportionate approach to sustainability information, it is appropriate to reserve a more granular assessment and disclosure to consensus mechanisms with more significant climate and other environment-related adverse impacts, especially where they exceed a certain level of energy consumption.
- (12) In addition to the key indicators, persons drawing up white papers and crypto-asset service providers should be able to voluntarily include, in a specific part of their disclosures, optional information on climate and other environment-related indicators that may be more complex to assess or for which it may be more difficult to find relevant data, for instance in relation to waste production and the use of natural resources.
- (13) In order to prevent greenwashing and to ensure the comparability of disclosures, these optional disclosures should be subject to the same harmonised rules on the presentation of information and on the methodologies as applicable to mandatory indicators. This applies, for instance, to other indirect GHG emissions (scope 3), such as upstream emissions linked to the equipment purchased by the DLT network nodes or downstream emissions related to waste management.
- (14) In order to foster consistency across disclosures in the absence of consensus on a specific set of reliable methodologies to calculate the identified indicators at this stage, harmonised principles should nonetheless apply to ensure comparability, avoid any methodological bias, and ensure their consistency with those referred to in the framework of the application of Directive (EU) 2022/2464 of the European Parliament and of the Council<sup>59</sup>. For instance, disclosures on energy consumption and GHG emissions should be aligned with the calculation guidance included in the Commission

---

<sup>59</sup> Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (OJ L 322, 16.12.2022, p. 15).

Delegated Regulation (EU) 2023/2772<sup>60</sup>. The methodology used to calculate each quantitative metric and deviations from this calculation guidance should be disclosed when applied.

- (15) In cases when information related to indicators is not available in a reasonable timeframe, estimates should be disclosed together with the reasonable assumptions used to calculate these estimates and details of the best efforts carried out to obtain the information. For instance, where the location of nodes cannot be identified as needed for certain disclosures, local, regional or global data should be used as necessary and appropriate, alongside details on the aforementioned best efforts.
- (16) The provisions of this Regulation are closely linked to each other, since they all deal with disclosures on climate and other environment-related impacts of consensus mechanisms that must be provided by persons drawing a white paper for asset-referenced tokens, e-money tokens and crypto-assets other than asset-referenced tokens and e-money tokens and by crypto-asset service providers for the crypto-assets in relation to which they provide services. In order to ensure consistency, coherence and comparability across these disclosures it is appropriate to include all the regulatory technical standards required by Articles 6(12), fourth subparagraph, 19(11), fourth subparagraph, 51(15), fourth subparagraph, and 66(6), fourth subparagraph of Regulation (EU) 2023/1114 into a single Regulation.
- (17) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA'), in cooperation with the European Banking Authority.
- (18) ESMA 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<sup>61</sup>,

HAS ADOPTED THIS REGULATION:

### *Article 1*

### **Definitions**

---

<sup>60</sup> Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards (OJ L, 2023/2772, 22.12.2023, ELI: [http://data.europa.eu/eli/reg\\_del/2023/2772/oj](http://data.europa.eu/eli/reg_del/2023/2772/oj)).

<sup>61</sup> 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).

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

- (a) 'incentive structure' means the set of incentives and penalties established as part of a consensus mechanism to economically incentivise distributed ledger technology (DLT) network nodes to co-operate in applying the rules and procedures of the consensus mechanism for the purpose of validating transactions in crypto-assets;
- (b) 'home Member State' means the home Member State as defined in Article 3(1), point (35)(f), of Regulation (EU) 2023/1114;
- (c) 'host Member State' means the host Member State as defined in Article 3(1), point (36), of Regulation (EU) 2023/1114;
- (d) 'greenhouse gas (GHG) emissions' means emissions of gases listed in Part 2 of Annex V to Regulation (EU) 2018/1999 of the European Parliament and of the Council<sup>62</sup> expressed in tonnes of CO<sub>2</sub>-equivalent;
- (e) 'climate and other environment-related indicators' means the indicators listed in the section 'Mandatory key indicator on energy consumption' of Table 2 of the Annex, in the section 'Supplementary key indicators on energy and GHG emissions' of Table 3 of the Annex, and in the section 'Optional indicators' of Table 4 of the Annex;
- (f) 'scope 1 DLT GHG emissions' means GHG emissions generated from sources that are controlled by the DLT network nodes applying the consensus mechanism;
- (g) 'scope 2 DLT GHG emissions' means GHG emissions from the consumption of purchased electricity, steam, or other sources of energy generated upstream from the DLT network nodes applying the consensus mechanism;
- (h) 'scope 3 DLT GHG emissions' means all indirect GHG emissions that are not covered by points (f) and (g) that occur in the value chain of the DLT network nodes applying the consensus mechanism, including both upstream and downstream emissions;
- (i) 'energy from renewable sources' or 'renewable energy' means energy from renewable sources or renewable energy as defined in Article 2, point (1), of Directive (EU) 2018/2001 of the European Parliament and of the Council<sup>63</sup>;
- (j) 'waste' means waste as defined in Article 2, point (23), of Directive (EU) 2018/2001;

---

<sup>62</sup> Regulation (EU) 2018/1999 of the European Parliament and of the Council of 11 December 2018 on the Governance of the Energy Union and Climate Action, amending Regulations (EC) No 663/2009 and (EC) No 715/2009 of the European Parliament and of the Council, Directives 94/22/EC, 98/70/EC, 2009/31/EC, 2009/73/EC, 2010/31/EU, 2012/27/EU and 2013/30/EU of the European Parliament and of the Council, Council Directives 2009/119/EC and (EU) 2015/652 and repealing Regulation (EU) No 525/2013 of the European Parliament and of the Council (OJ L 328, 21.12.2018, p.1).

<sup>63</sup> Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast) (OJ L 328, 21.12.2018, p. 82).

- (k) 'waste electrical and electronic equipment' or 'WEEE' means waste electrical or electronic equipment as defined in Article 3(1), point (e), of Directive 2012/19/EU of the European Parliament and of the Council<sup>64</sup>;
- (l) 'non-recycled waste' means any waste not recycled within the meaning of 'recycling' in Article 3, point 17, of Directive 2008/98/EC of the European Parliament and of the Council<sup>65</sup>;
- (m) 'hazardous waste' means hazardous waste as defined in Article 3, point 2, of Directive 2008/98/EC;
- (n) 'natural resources' means natural resources as defined in Table 2 of Annex II to the Commission Delegated Regulation (EU) 2023/2772.

## *Article 2*

### **Presentation of information in the white papers**

Persons drawing up the crypto-asset white paper referred to in Articles 6, 19 or 51 of Regulation (EU) 2023/1114 shall ensure that the information in the crypto-asset white papers disclosed in accordance with this Regulation complies with Articles 1 to 3 of Commission Implementing Regulation (EU) 2024/XXX of XXXX laying down implementing technical standards for the application of Regulation (EU) No 2023/1114 with regard to forms, formats and templates for the crypto-asset white papers<sup>66</sup>.

## *Article 3*

### **General principles for the presentation of information by crypto-asset service providers**

1. Crypto-asset service providers shall make publicly available on their website the information required by this Regulation free of charge, in a downloadable file, in a way that is easy to read, using characters of readable size and using a style of writing that facilitates its understanding.
2. Crypto-asset service providers shall review and update the information published on their websites in accordance with this Regulation on a regular basis, at least annually, and update the information without undue delay in case of material changes, by providing clear

---

<sup>64</sup> Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) (OJ L 197, 24.7.2012, p. 38).

<sup>65</sup> Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).

<sup>66</sup> [●]

evidence of the changes made. They shall clearly mention the date of publication of the information and the date of the latest review or update.

3. The disclosure made in accordance with this Regulation shall allow the public to compare the adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanisms and their incentive structures across all the crypto-assets in relation to which the crypto-asset service provider provides crypto-asset services.
4. The disclosures referred to in this Regulation shall be made available by the crypto-asset service provider in at least one of the official languages of the Member State where the crypto-asset service provider has its registered office, or in a language customary in the sphere of international finance.

Where the crypto-asset service provider is providing crypto-assets services with respect to a specific crypto-asset in a Member State other than its home Member State, the disclosures referred to in this Regulation for that crypto-asset shall also be made available in an official language of that host Member State, or in a language customary in the sphere of international finance.

#### *Article 4*

##### **Disclosures in the white papers**

1. Persons drawing up the crypto-asset white paper referred to in Articles 6, 19 or 51 of Regulation (EU) 2023/1114 shall provide in the white paper the information on the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue crypto-assets referred to in Table 2 of the Annex in the format set out therein.
2. The persons referred to in paragraph 1 shall also provide in the white paper the information referred to in Table 3 of the Annex, in the format set out therein, where the yearly energy consumption as reported in field S.8 of Table 2 exceeds 500 000 kilowatt-hours.

Where the condition in the first subparagraph of this paragraph is not met, the persons referred to in paragraph 1 may provide in the white paper information on one or more of the indicators listed in Table 3 of the Annex, in the format of the templates set out therein. When providing in the white paper information on one or more of the indicators referred to in the section 'Supplementary key indicators on energy and GHG emissions' referred to in Table 3 of the Annex, the persons referred to in paragraph 1 shall also provide the corresponding information listed in the section on 'Sources and methodologies' of the same Table.

3. The persons referred to in paragraph 1 may provide in the white paper information on one or more of the indicators listed in Table 4 of the Annex, in the format set out therein. When providing in the white paper information on one or more of the indicators listed in the section 'Optional indicators' of Table 4 of the Annex, the persons referred to in paragraph 1 shall

provide also the corresponding information listed in the section on ‘Sources and methodologies’ of the same Table.

#### *Article 5*

##### **Disclosures on the websites of crypto-assets service providers**

1. Crypto-asset service providers shall provide on their website, in relation to crypto-assets for which they provide crypto-asset services, the information on the principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue crypto-assets referred to in Table 2 of the Annex, in the format set out therein.
2. Crypto-asset service providers shall provide on their website, in relation to crypto-assets for which they provide crypto-asset services, the information referred to in Table 3 of the Annex, in the format set out therein, where both the following conditions are met:
  - (a) the crypto-asset service provider provides one or more of the services referred to in Article 3(16), points (b), (c) and (d) of Regulation (EU) 2023/1114;
  - (b) the yearly energy consumption as reported in field S.8 exceeds 500,000 kilowatt-hours.

Where the conditions listed in points (a) and (b) of the first subparagraph of this paragraph are not met, the crypto-asset service provider may provide on their website information on one or more of the indicators referred to in Table 3 of the Annex, in the format set out therein. When providing information on one or more of the indicators referred to in the section ‘Supplementary key indicators on energy and GHG emissions’ of Table 3 of the Annex, crypto-asset service providers shall also provide on their website the corresponding information referred to in the section on ‘Sources and methodologies’ of the same Table.

3. Crypto-asset service providers may provide on their website, in relation to crypto-assets for which they provide crypto-assets services, information on one or more of the indicators referred to in Table 4 of the Annex, in the format set out therein. When providing information on one or more of the indicators referred to in the section ‘Optional indicators’ of Table 4 of the Annex, crypto-asset service providers shall provide on their website the corresponding information referred to in the section on ‘Sources and methodologies’ of the same Table.

#### *Article 6*

##### **Rules on the disclosures**

1. Persons referred to in paragraph 1 of Article 4 and crypto-asset service providers, in relation to crypto-assets for which they provide crypto-asset services, shall disclose in the section ‘General information’ in Table 2 of the Annex all of the following information:



- (a) their name and their legal entity identifier as reported, respectively pursuant to the [ITS on standard forms and templates for the crypto-asset white paper] or to the [RTS on authorisation of crypto-asset service providers];
  - (b) information on the features of the consensus mechanisms used for the validation of transactions and for the maintenance of the integrity of the distributed ledger of transactions and the incentive structure as reported pursuant to [ITS on standard forms and templates for the crypto-asset white paper];
  - (d) the reference period of the statement, and the period for which estimates are used.
2. Where, pursuant to Article 66(5) of Regulation (EU) 2023/1114, crypto-asset service providers use information obtained from crypto-asset white papers in order to comply with Article 4 of this Regulation, they shall provide the name and relevant identifier of the person drawing up that white paper in the section on ‘Sources and methodologies’ of the relevant Table of the Annex.
  3. Where the information referred to in Tables 2, 3 or 4 of the Annex was subject to a verification by one or more third parties, persons referred to in paragraph 1 of Article 4 and crypto-asset service providers shall indicate it and provide the name or names of such third parties in the section on ‘Sources and methodologies’ of the relevant Table of the Annex.
  4. The methodologies used to calculate the climate and other environment-related indicators shall be rigorous, systematic, objective, capable of validation and applied continuously.

The information referred to in fields S.8 of Table 2 of the Annex, in fields S.10 and S.11 of Table 3 of the Annex, and in fields S.17 and S.18 of Table 4 of the Annex shall be calculated in accordance with the calculation guidance in point AR 32 of the Appendix A of the ESRS E1 in Annex I to Commission Delegated Regulation (EU) 2023/2772.

The information referred to in fields S.12, S.13 and S.14 of Table 3 of the Annex, and in fields S.19, S.20 and S.21 of Table 4 of the Annex shall be calculated in accordance with the calculation guidance in points AR 39, 43, 45, 46 and 47 of the Appendix A of the ESRS E1 in Annex I of Commission Delegated Regulation (EU) 2023/2772.

5. Where DLT network nodes use mechanisms to off-set their energy consumption and GHG emissions, the use of these mechanisms may be separately disclosed in the section ‘Sources and methodologies’ of Tables 2, 3 and 4 of the Annex. The effect of such off-setting mechanisms shall not be taken into account when calculating the climate and other environment-related indicators.
6. Where the information relating to the climate and other environment-related indicators is not readily available, the persons referred to in paragraph 1 of Article 4 and crypto-asset service providers shall provide estimates, together with details of the best efforts carried out to obtain the information by conducting additional research, cooperating with third party data providers or external experts or making reasonable assumptions.



The persons referred to in paragraph 1 of Article 4 and crypto-asset service providers shall include the details of the best efforts referred to in the first subparagraph of this paragraph in the section on ‘Sources and methodologies’ of Tables 2, 3 and 4 of the Annex, including by disclosing:

- (a) the fact that estimates have been used and a clear indication of which sustainability indicators are provided based on estimates; and
  - (b) the methodology used to calculate the climate and other environment-related indicators, including a description of deviations from the calculation guidance referred to in the second and third subparagraphs of paragraph 4 of this Article and an explanation of the reasons for such deviations, and the main assumptions and precautionary principles underlying those estimates;
7. The persons referred to in paragraph 1 of Article 4 and crypto-asset service providers may provide in the section on ‘Sources and methodologies’ of Tables 2, 3 and 4 of the Annex the following information:
- (a) the methodology to estimate missing, unreported, or underreported metrics;
  - (b) the external data-sets used in the estimation of missing, unreported or underreported metrics;
  - (c) the name and a hyperlink to the website of the external provider of the data on which the estimates are based, where relevant; and
  - (d) the methodology used to offset their energy consumption in accordance with paragraph 5 of this Article, where relevant.

Where any information referred to in points (a) to (d) of the first subparagraph of this paragraph is not included, the person referred to in paragraph 1 of Article 4 or the crypto-asset service provider shall indicate it in a clear manner.

## *Article 7*

### **Entry into force and application**

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,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

*ANNEX*

**Template for the presentation of the information on principal adverse impacts on the climate and other environment-related adverse impacts in the crypto-asset white paper and on the website of a crypto-asset service provider**

*Table 1*

**Legend for Tables 2, 3 and 4**

<b>SYMBOL</b>	<b>DATA TYPE</b>	<b>DEFINITION</b>
{DATEFORMAT}	ISO 8601 date format	Dates shall be formatted in the following format: YYYY-MM-DD.
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	Numerical field for both positive and negative values.  Decimal separator is '.' (full stop);  Negative numbers are prefixed with '-' (minus);  Values are rounded and not truncated.

*Table 2*

**Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism**

<b>N</b>	<b>Field</b>	<b>Content to be reported</b>	<b>Format and standards to be used</b>
<b>General information</b>			
S.1	Name	Name reported in field A.1, B.2 or C.1 of table 2 of the Annex II to the [Implementing Regulation (EU) 2024/XXX on standard forms and templates for the crypto-asset white paper], in field A.1 of table 3 or table 4 of that Annex, or name of the crypto-asset service provider	Free alphanumerical text
S.2	Relevant legal entity identifier	Identifier referred to in field A.2, B.3 or C.2 of table 2 of the Annex II to the [Implementing Regulation (EU) 2024/XXX on standard forms and templates for the crypto-asset white paper], in field A.3 of table 3 or table 4 of that Annex, or identifier of the crypto-asset service provider referred to in Article XX of the [Delegated Regulation (EU) 2024/XXX on authorisation of crypto-asset service providers]	Free alphanumerical text
S.3	Name of the crypto-asset	Name of the crypto-asset, as reported in field D.2 of table 2 of the Annex II to the [Implementing Regulation (EU) 2024/XXX on standard forms and templates for the crypto-asset white paper], in field B.1 of table 3 or table 4 of that Annex, where relevant	Free alphanumerical text

S.4	Consensus Mechanism	The consensus mechanism, as reported in field H.4 of table 2 of the Annex II to the [Implementing Regulation (EU) 2024/XXX on standard forms, formats and templates for the crypto-asset white paper], in field E.4 of table 3 of that Annex, in field E.5 of table 4 of that Annex, where relevant, including the information referred to in Article 6(1), point (b) of this Regulation.	Free alphanumerical text
S.5	Incentive Mechanisms and Applicable Fees	<p>Incentive mechanisms to secure transactions and any fees applicable, as reported in field H.5 of table 2 of the Annex II to the [Implementing Regulation (EU) 2024/XXX on standard forms and templates for the crypto-asset white paper], in field E.5 of table 3 of that Annex, in field E.6 of table 4 of that Annex, where relevant.</p> <p>For persons drafting a crypto-asset white paper pursuant to Articles 6, 19 or 51 of Regulation (EU) 2023/1114, the information may be provided by including a cross-reference to the aforementioned fields.</p>	Free alphanumerical text
S.6	Beginning of the period to which the disclosure relates	Beginning of the period to which the disclosure relates	{DATEFORMAT}
S.7	End of the period to which the disclosure relates	End of the period to which the disclosure relates	{DATEFORMAT}
<b>Mandatory key indicator on energy consumption</b>			
S.8	Energy consumption	Total amount of energy used for the validation of transactions and the maintenance of the integrity of the	Amount in kilowatt-hours (kWh) {DECIMAL-18/5}

		distributed ledger of transactions, expressed per calendar year	
<b>Sources and methodologies</b>			
S.9	Energy consumption sources and methodologies	Sources and methodologies used in relation to the information reported in field S.8	Free alphanumerical text

*Table 3*

**Supplementary information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism**

<b>Supplementary key indicators on energy and GHG emissions</b>			
S.10	Renewable energy consumption	Share of energy used generated from renewable sources, expressed as a percentage of the total amount of energy used per calendar year, for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions.	Percentage {DECIMAL-11/10}
S.11	Energy intensity	Average amount of energy used per validated transaction	Amount in kWh {DECIMAL-18/5}
S.12	Scope 1 DLT GHG emissions – Controlled	Scope 1 GHG emissions per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	Amount in tonnes (t) carbon dioxide equivalent (CO <sub>2</sub> e) {DECIMAL-18/5}
S.13	Scope 2 DLT GHG emissions – Purchased	Scope 2 GHG emissions, expressed in tCO <sub>2</sub> e per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	Amount in tCO <sub>2</sub> e {DECIMAL-18/5}

S.14	GHG intensity	Average GHG emissions (scope 1 and scope 2) per validated transaction	Amount in kilogram (kg) CO <sub>2</sub> e (Tx) {DECIMAL-18/5}
<b>Sources and methodologies</b>			
S.15	Key energy sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.10 and S.11	Free alphanumerical text
S.16	Key GHG sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.12, S.13 and S.14	Free alphanumerical text

*Table 4*

**Optional information on principal adverse impacts on the climate and on other environment-related adverse impacts of the consensus mechanism**

N	Field	Content to be reported	Format and standards to be used
<b>Optional indicators</b>			
S.17	Energy mix	Description of the relative contributions of each different primary energy source used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed as percentages	Percentage {DECIMAL-11/10}



S.18	Energy use reduction	Energy use reduction targets or commitments, expressed in absolute or relative reduction of energy use over one calendar year	Amount in kWh {DECIMAL-18/5} or Percentage {DECIMAL-11/10}
S.19	Carbon intensity	Carbon intensity of the energy used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	Amount in kgCO <sub>2</sub> e per kWh {DECIMAL-18/5}
S.20	Scope 3 DLT GHG emissions - Value chain	Scope 3 GHG emissions for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions per calendar year	Amount in tCO <sub>2</sub> e {DECIMAL-18/5}
S.21	GHG emissions reduction targets or commitments	GHG emissions reduction targets or commitments, expressed in terms of absolute or relative reduction in GHG emissions over one calendar year	Free alphanumerical text
S.22	Generation of waste electrical and electronic equipment (WEEE)	Total amount of WEEE generated for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions per calendar year	Amount in t {DECIMAL-18/5}
S.23	Non-recycled WEEE ratio	Share of the total amount of WEEE generated for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, not recycled per calendar year	Percentage {DECIMAL-11/10}
S.24	Generation of hazardous waste	Total amount of hazardous waste generated for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions per calendar year	Amount in t {DECIMAL-18/5}

S.25	Generation of waste (all types)	Total amount of waste generated by the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	Amount in t {DECIMAL-18/5}
S.26	Non-recycled waste ratio (all types)	Share of the total amount of waste generated for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions not recycled per calendar year	Percentage {DECIMAL-11/10}
S.27	Waste intensity (all types)	Total amount of waste generated per transaction validated	Amount in grams (g) per Tx {DECIMAL-18/5}
S.28	Waste reduction targets or commitments (all types)	Waste reduction targets or commitments, expressed in absolute or relative reduction in waste generation over one calendar year	Free alphanumerical text
S.29	Impact of the use of equipment on natural resources	Description of the impact on natural resources of the production, the use and the disposal of the devices of the DLT network nodes	Free alphanumerical text
S.30	Natural resources use reduction targets or commitments	Natural resources use reduction targets or commitments, expressed in absolute or relative reduction in use of natural resources over one calendar year	Free alphanumerical text
S.31	Water use	Total water consumption linked to the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed in cubic meters	Amount in cubic meters {DECIMAL-18/5}
S.32	Non recycled water ratio	Share of the total water consumed not recycled and not reused linked to the validation of transactions and the	Percentage {DECIMAL-11/10}

		maintenance of the integrity of the distributed ledger of transactions per calendar year, expressed as a percentage	
<b>Sources and methodologies</b>			
S.33	Other energy sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.17 and S.18	Free alphanumerical text
S.34	Other GHG sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.19, S.20 and S.21	Free alphanumerical text
S.35	Waste sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.22, S.23, S.24, S.25, S.26, S.27 and S.28	Free alphanumerical text
S.36	Natural resources sources and methodologies	Sources and methodologies used in relation to the information reported in fields S.29, S.30, S.31 and S.32	Free alphanumerical text

## 8.5 Annex V: Draft RTS pursuant to Article 68(10)(a) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

**supplementing Regulation (EU) No 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) No 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<sup>67</sup>, and in particular Article 68(10), point (a) thereof,

Whereas:

- (1) Ensuring continuity and regularity in the performance of crypto-asset services is imperative to maintain orderly conditions in the crypto-asset market and to protect investors from adverse disruptions that may affect their investments. To maintain the resilience of their critical or important functions and hence the availability of their services, crypto-asset service providers should establish adequate governance arrangements for compliance, staffing, and outsourcing. As part of their organisational requirements, crypto-asset service providers should employ management and staff with adequate knowledge, skills, and expertise to perform their functions, including through the preparation of a business continuity policy and implementation of business continuity plans.
- (2) Articles 11 and 12 of Regulation (EU) 2022/2554 of the European Parliament and of the Council<sup>68</sup> provide for requirements relating to response and recovery, backup policies and procedures, restoration and recovery procedures and methods concerning the ICT systems of crypto-asset services providers. The [*Delegated Regulation (EU) xx/xxx on DORA ICT risk management framework*] further specifies components of the ICT business continuity policy, the testing of ICT business continuity plans, the

---

<sup>67</sup> OJ L 150, 9.6.2023, p.40.

<sup>68</sup> 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).

components of the ICT response and recovery plans of crypto-asset service providers. This Regulation complements those provisions of Regulation (EU) 2022/2554 and of *Delegated Regulation (EU) xx/xxx on DORA ICT risk management framework*] with respect to continuity and regularity in the performance of the crypto-asset services.

- (3) Certain measures taken by a crypto-asset service provider may not be capable of ensuring the regularity and continuity of their services when disruptions occur which are caused by problems inherent in the operation of the distributed ledger that the crypto-asset service provider does not control, such as permissionless distributed ledgers. To limit the adverse impact on clients affected by disruptions to services using a permissionless distributed ledger, the crypto-asset service provider should include measures for timely communication with clients and other external stakeholders in their business continuity plans. Such communication should include essential and timely information for clients, including ongoing status updates until the incident is resolved and services are resumed. In order to ensure that clients and stakeholders have as comprehensive information as possible, 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, it should nevertheless communicate updates to clients and other stakeholders on a best effort basis.
- (4) To avoid excessive or disproportionate administrative burden for small and medium-enterprises (SMEs) and start-ups that would fall under the scope of this Regulation, crypto-asset service providers should consider the scale, nature, and range of their services provided in their business continuity arrangements. The specific business continuity requirements for crypto-asset service providers should be determined by means of a robust self-assessment. Crypto-asset service providers should include in their self-assessment the criteria listed in the Annex of this Regulation. That self-assessment should include any other circumstances not expressly set out that may have an impact on the crypto-asset service provider.
- (5) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (6) ESMA 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<sup>69</sup>,

---

<sup>69</sup> 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).

HAS ADOPTED THIS REGULATION:

*Article 1*

**Definitions**

1. 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<sup>70</sup>.
  - (b) 'permissionless distributed ledger' means a type of distributed ledger as defined under Article 3(1) point 2 of Regulation (EU) 2023/1114 in which no entity controls the distributed ledger and DLT network nodes can be set up by any persons complying with the technical requirements and the protocols.

*Article 2*

**Business continuity organisational arrangements**

1. Crypto-asset service providers shall have adequate resources in charge of adopting and implementing the plans, procedures, and measures that comprise the business continuity policy specified in Article 3.
2. The crypto-asset service provider's management body shall define and endorse the plans, procedures, and measures that comprise the business continuity policy. The crypto-asset service provider's management body shall also be responsible for the implementation of the business continuity policy, and for reviewing its effectiveness on at least an annual basis.
3. Crypto-asset service providers shall establish adequate procedures, including effective internal communication channels, to ensure that updated information on business continuity arrangements is transmitted to all relevant internal staff.

---

<sup>70</sup> 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).

### *Article 3*

#### **Business continuity policy**

1. Crypto-asset service providers shall be able to demonstrate at all times that the systems critical to the operation of their business functions have sufficient stability by having an effective business continuity policy to address disruptive incidents or performance issues. The business continuity policy shall be documented in a durable medium and periodically reviewed in accordance with Article 2(2).
2. Crypto-asset service providers shall include in the business continuity policy all of the following:
  - (a) a definition of the scope, including 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;
  - (c) provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the business continuity policy and to ensure that sufficient resources are available;
  - (d) provisions on the alignment between the general business continuity plans and the ICT-specific business continuity plans, and ICT response and recovery plans referred to in [Articles 26 and 27 of Delegated Regulation (EU) xx/xxx on DORA ICT risk management framework];
  - (e) provisions on the review of the effectiveness of the implemented business continuity plans, in accordance with Article 5(2).

### *Article 4*

#### **Business continuity plans**

1. Crypto-asset service providers shall establish business continuity plans to implement the business continuity policy provided for in Article 3. The business continuity plans shall set out the procedures for managing disruptive incidents. The business continuity plans shall support objectives to protect and, where necessary, re-establish the confidentiality, integrity, and availability of client data, and availability of the business functions, supporting processes and information assets of the crypto-asset service providers.
2. The business continuity plans shall provide for the following minimum content:



- (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 or data centres or loss or alteration of critical data and documents;
  - (b) the procedures and policies to be followed in case of a disruptive event, including necessary measures to recover critical or important functions consistent with recovery time objectives and recovery point objectives and the maximum time to resume services;
  - (c) 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 and between the crypto-asset service provider and the infrastructures on which its services rely;
  - (e) procedures for timely communications with clients and other external stakeholders.
3. For the purposes of point (e) of paragraph 2, the procedures shall cover in detail the process to be followed 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 crypto-asset service provider shall ensure that the communication to clients and external stakeholders includes information on when the services are expected to be resumed, on the reasons and the impact of the incident, and on risks concerning clients' funds and crypto-assets held on their behalf. Where this information is not readily available, the crypto-asset service provider shall communicate updates to clients and external stakeholders on a best effort basis.
4. The business continuity plans shall set out 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 on the basis of realistic scenarios the operation of the business continuity plans in Article 4. 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) (b).

2. Crypto-asset service providers shall test the business continuity plans at least once a year taking into account the results of the tests, the most recent threat intelligence, lessons derived from previous events and, where relevant, any changes in the recovery objectives, including recovery time objectives and recovery point objectives, or changes in the business functions.
3. Crypto-asset service providers shall document in writing and store the results of the testing activity and submit them to the crypto-asset service provider's management body as well as to the operating units involved in the business continuity plans.
4. Crypto-asset service providers shall ensure that testing of the business continuity plans does not interfere with normal conduct of services.

#### *Article 6*

#### **Complexity and risk considerations**

1. In establishing the business continuity policy, and the related plans, procedures and measures, crypto-asset service providers shall take into account elements of increased complexity or risk, including the type and range of crypto-asset services offered, the extent to which their services rely on permissionless distributed ledger and the potential impact of the 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, at least once a year, carry out a self-assessment of the scale, the nature and range of their services. The self-assessment shall analyse the applicable criteria set out in the Annex to this Regulation and any other criteria that the crypto-asset service provider considers relevant.

#### *Article 7*

#### **Entry into force and application**

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,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

*ANNEX*

**Criteria for the self-assessment of crypto-asset service providers**

- (a) Nature of the crypto-asset service provider, by assessing the following elements:
- (i) the class designation in accordance with Annex IV of Regulation (EU) No 2023/1114;
  - (ii) the average liquidity levels or market depth of crypto-assets available to trade on a trading platform for crypto-assets, where applicable;
  - (iii) the role of the crypto-asset service provider in the financial system, including whether the crypto-asset service provider operates a trading platform for crypto assets and whether crypto-assets traded on its platform are traded on other trading platforms for crypto-assets.
- (b) Scale, by assessing the impact of the crypto-asset service provider on the orderly functioning of the markets based on at least the following elements, where applicable:
- (i) whether the crypto-asset service provider qualifies as significant in accordance with Article 85 of Regulation (EU) No 2023/1114;
  - (ii) the number of countries in which the crypto-asset service provider is conducting business activity;
  - (iii) the number of clients;
  - (iv) the number of active users;
  - (v) the value of crypto-assets held in custody;
  - (vi) the volume of transactions on a trading platform for crypto-assets;
  - (vii) the number of transfers of crypto-assets conducted on behalf of clients;
  - (viii) the number of orders executed on behalf of clients.
- For the purposes of points (iii) to (viii) of point (b), the crypto-asset service provider shall use for the self-assessment the daily average over a one-year reference period.
- (c) Complexity, by assessing the following elements, where applicable:

- (i) the structure of the crypto-asset service provider in terms of ownership and governance and its organisational, operational, technical, physical, and geographical presence;
- (ii) the level of outsourcing of the crypto-asset service provider and in particular where any critical or important operational functions have been outsourced;
- (iv) the number and type of distributed ledgers used in the execution of services;
- (v) the number of DLT network nodes the crypto-asset service provider operates on one or multiple distributed ledger(s);
- (vi) the number and type of smart contracts deployed and maintained by the crypto-asset service provider;
- (vii) how the private cryptographic keys of clients or other means of accessing crypto-assets are secured under safekeeping;
- (viii) the use of software and hardware-based custodial wallets or wallets that secure cryptographic keys using multiple fiduciaries.

## 8.6 Annex VI: Draft RTS pursuant to Article 76(16)(a) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

**supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the manners in which transparency data for crypto-asset service providers operating a trading platform for crypto-assets is to be presented**

**(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<sup>71</sup>, and in particular Article 76(16), first subparagraph, point (a) thereof,

Whereas:

- (1) A high degree of transparency is essential to ensure that investors are adequately informed as to the true level of actual and potential transactions in crypto-assets traded on a trading platform operated by a crypto-asset service provider. This high degree of transparency should also ensure a level playing field between trading platforms so that the price discovery process in respect of particular crypto-assets is not impaired by the fragmentation of liquidity, and investors are not thereby penalised.
- (2) In order for investors to be adequately informed about access, costs, scope, functioning of trading platforms they use or intend to use, it is important for trading platforms to make available their operating rules in a transparent and non-discriminatory manner. Investors should have easy access to this information.
- (3) Trading platforms for crypto-assets should publicly disclose all orders on a continuous basis and transactions as close to real-time as is technically possible on their platforms. It is important to harmonise the information to be published so as to allow investors to use, compare and aggregate the information published from different trading platforms for crypto-assets.

---

<sup>71</sup> OJ L 150, 9.6.2023, p. 40.

- (4) In order to ensure a level playing field between all types of investors, both qualified investors and retail holders, regarding the access to order management facilities, trading platforms for crypto assets may offer reserve and stop orders directly through their trading platform when certain conditions are met in accordance with this Regulation.
- (5) Given the rapidly evolving landscape of the crypto-asset market, this regulation should cater for the different operational frameworks for Centralised Exchanges (CEXs) and on-chain Decentralised Exchanges (DEXs). CEXs, characterised by centralised control over trading operations and custodial practices, utilise mechanisms such as central limit order books (CLOB), which are common in traditional finance, distinguishing them from DEXs, which operate without central operator and facilitate trading directly on the blockchain through smart contracts, also working with self-custody wallets mechanisms. In addition, the evolving landscape that includes hybrid models combining features of both CEXs and DEXs necessitates a regulatory approach that is both precise and adaptable, ensuring clear legal distinctions are articulated. With respect to the abovementioned centralised, decentralised and hybrid models, it is therefore appropriate to clarify the transparency data applicable to those trading systems that would normally be available in an on-chain context, in as much as they are not operated in a fully decentralised manner without intermediary and hence subject to Regulation (EU) 2023/1114. For instance, in the case of Automated Market Maker (AMM) models which do not operate in a fully decentralised manner without intermediary, this would include the mathematical formula used to determine the price in the liquidity pool and, if applicable, a price simulator.
- (6) Information which is required to be made available as close to real time as possible should be made available as instantaneously as technically feasible, assuming a reasonable level of efficiency of the systems of the crypto-asset service providers operating a trading platform for crypto-assets. The publication of the information close to the maximum time limit should occur only in exceptional cases where the systems available do not allow for a publication in a shorter period of time.
- (7) It is necessary to specify the level of disaggregation by which trading platforms should be able to sell data. Crypto-asset service providers operating a trading platform for crypto-assets should disaggregate data by, as a minimum, the type of crypto-asset (asset-referenced tokens, e-money tokens, crypto-assets other than asset-referenced tokens and e-money tokens), the currency in which the crypto-assets are traded, and the type of trading system. This data should be available on a crypto-asset basis when available.
- (8) To ensure that pre-trade and post-trade data offered for purchase appropriately matches the demand from market participants, crypto-asset service providers operating a trading platform should offer any combination of the disaggregation criteria on a reasonable commercial basis.



- (9) In order to identify crypto-assets consistently, an international standard identifier for digital tokens as the Digital Token Identifier issued by the Digital Token Identifier Foundation (DTIF) should be used. This identifier is appropriate as it follows the principles of uniqueness, neutrality, reliability, open source, scalability, accessibility on a cost-recovery basis and is offered under an appropriate governance framework. Where the DTI is not used, an identifier that ensures similar characteristics and complies with the standard set out in [*Delegated Regulation (EU) xx/xxx on record keeping for crypto-asset service providers*]<sup>72</sup> should be used.
- (10) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (11) ESMA 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<sup>73</sup>,

HAS ADOPTED THIS REGULATION:

#### Article 1

### **General principles of presentation of the information on operating rules for trading platforms**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall publish the information on the operating rules for their trading platform free of charge and in a manner that is easily accessible, non-discriminatory, prominent, comprehensible, fair, clear and not misleading.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall present the information on operating rules for trading platforms in a way that is easy to read and use a style that facilitates its understanding.
3. Crypto-asset service providers operating a trading platform for crypto-assets shall make available the operating rules for their trading platform in a single document and publish them on the crypto-asset service provider's website.

---

<sup>72</sup> [...]

<sup>73</sup> 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).

## Article 2

### **Pre-trade transparency**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall make public the range of bid and offer prices and the depth of trading interest at those prices, in accordance with the type of trading systems they operate as listed in Table 1 of Annex I.
2. With respect to orders which meet all of the following conditions:
  - (a) are contingent on the occurrence of objective market conditions which are pre-defined by the trading system's protocol;
  - (b) cannot interact with other trading interests prior to disclosure to the order book operated by the trading platform;
  - (c) once disclosed to the order book, interact with other orders in accordance with the rules applicable to orders of that kind at the time of disclosure,crypto-asset service providers operating a trading platform for crypto-assets shall make such orders public when the pre-determined market condition in point (a) materialises.
3. Crypto-asset service providers operating a trading platform for crypto-assets shall make public the details of each order as set out in Tables 2 and 3 of Annex I.

## Article 3

### **Post-trade transparency**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall make public the details of each transaction as set out in Tables 1 and 2 of Annex II.
2. Where a previously published trade report is cancelled, crypto-asset service providers operating a trading platform for crypto-assets shall make public a new trade report which contains all the details of the original trade report and the cancellation flag specified in Table 3 of Annex II.
3. Where a previously published trade report is amended, crypto-asset service providers operating a trading platform for crypto-assets shall make the following information public:
  - (a) a new trade report that contains all the details of the original trade report and the cancellation flag specified in Table 3 of Annex II;
  - (b) a new trade report that contains all the details of the original trade report with all necessary details corrected and the amendment flag specified in Table 3 of Annex II.

## Article 4

### **Real time publication of transactions**

For transactions executed on their crypto-asset trading platforms, crypto-asset service providers operating a trading platform for crypto-assets shall make public the details of each transaction as set out in Tables 1, 2 and 3 of Annex II as close to real-time as is technically possible and in any case within thirty seconds after the execution of the transaction.

## Article 5

### **Disaggregation of pre-trade and post-trade data**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall make the information published in accordance with Articles 2 and 3 available to the public by publishing pre-trade and post-trade transparency data separately.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall upon request make the information published in accordance with Articles 2 and 3 available to the public by presenting pre-trade and post-trade data disaggregated for each crypto-asset.
3. In addition to presenting the data in accordance with paragraph 2, crypto-asset service providers operating a trading platform may present the data referred to in paragraph 2 in bundles of crypto-assets.
4. Paragraphs 1 to 3 shall not apply where the information referred to in Articles 2 and 3 is made available free of charge.

## Article 6

### **Entry into force and application**

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,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

ANNEX I

**Pre-trade information to be made public**

*Table 1*

**Description of the type of trading systems and the related information to be made public in accordance with Article 1**

	<b>Type of trading system</b>	<b>Description of the trading system</b>	<b>Information to be made public</b>
<b>1</b>	Continuous auction order book trading system	A system that by means of an order book and a trading algorithm operates without human intervention and matches sell orders with buy orders on the basis of the best available price on a continuous basis.	The aggregated number of orders and the crypto-assets that they represent at each price level for at least the five best bid and offer price levels.
<b>2</b>	Quote-driven trading system	A system where transactions are concluded on the basis of firm quotes that are continuously made available to participants.	<p>The best bid and offer by price of each participant in crypto-assets traded on the trading system, together with the volumes attaching to those prices.</p> <p>The quotes made public shall be those that represent binding commitments to buy and sell the crypto-assets and which indicate the price and volume of crypto-assets in which the participants are prepared to buy or sell.</p>
<b>3</b>	Periodic auction trading system	A system that matches orders on the basis of a periodic auction and a trading algorithm operated without human intervention.	The price at which the auction trading system would best satisfy its trading algorithm in respect of crypto-assets traded on the trading system and the volume that would potentially be

			executable at that price by participants in that system.
4	Automated market makers	A system relying on liquidity pools and mathematical pricing and valuation models for the automatic execution of individual transactions.	<p>(i) The mathematical equation used to determine the price and the quantity of the crypto-assets in the liquidity pools;</p> <p>(ii) the level of liquidity in the liquidity pool at a given moment in time (on a continuous basis); and</p> <p>(iii) any further information and parameters that allow to determine the price at which a specific order would be executed.</p>
5	Hybrid trading system	A system falling into two or more of the types of trading systems referred to in rows 1 to 4 of this table.	<p>For hybrid trading systems that combine different trading systems at the same time, the requirements correspond to the pre-trade transparency requirements applicable to each type of trading system that forms the hybrid system.</p> <p>For hybrid trading systems that combine two or more trading systems subsequently, the requirements correspond to the pre-trade transparency requirements applicable to the respective trading system operated at a particular point in time</p>
6	Any other trading system	Any other type of trading system.	Adequate information as to the level of orders or quotes and of trading interests in respect of crypto-assets traded on the trading system; in particular, the five best bid and offer price levels and/or two-way quotes of each market maker in the crypto-

			assets, if the characteristics of the price discovery mechanism so permit.
--	--	--	--

Table 2

Symbol table for Table 3

SYMBOL	DATA TYPE	DEFINITION
{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{CURRENCYCODE_3}	3 alphanumerical characters	3 letter currency code, as defined by ISO 4217 currency codes
{DATE_TIME_FORMAT}	ISO 8601 date and time format	<p>Date and time in the following format:            YYYY-MM-DDThh:mm:ss.dddddZ.</p> <ul style="list-style-type: none"> <li>– ‘YYYY’ is the year;</li> <li>– ‘MM’ is the month;</li> <li>– ‘DD’ is the day;</li> <li>– ‘T’ – means that the letter ‘T’ shall be used               <ul style="list-style-type: none"> <li>– ‘hh’ is the hour;</li> <li>– ‘mm’ is the minute;</li> </ul> </li> <li>– ‘ss.ddddd’ is the second and its fraction of a second;               <ul style="list-style-type: none"> <li>– Z is UTC time.</li> </ul> </li> </ul> <p>Dates and times shall be reported in UTC.</p>
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	<p>Numerical field for both positive and negative values.</p> <ul style="list-style-type: none"> <li>– decimal separator is ‘.’ (full stop);</li> </ul> <p>negative numbers are prefixed with ‘-’ (minus);            Values are rounded and not truncated.</p>
{MIC}	4 alphanumerical characters	Market identifier as defined in ISO 10383



Table 3

**List of details for the purpose of pre-trade transparency**

#	Field identifier	Description and details to be published	Format to be populated as defined in Table 2
1	Submission date and time	Where the orders and quotes do not have to be published on an aggregated basis, the date and time when the order or quote was introduced for execution into the trading system.	{DATE_TIME_FORMAT}
2	Crypto-asset identification code	Unique and unambiguous identifier of the crypto-asset in accordance with Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].	To be populated in accordance with Field 10 of table 2 of section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].
3	Crypto-asset full name	Full name of the crypto-asset.	{ALPHANUM-350}
4	Buy-sell indicator	Indicator of whether the order is to buy or sell.	'BUYI' — buy  'SELL' — sell
5	Price	<p>The price of orders and quotes as required for each trading system in Table 1 of Annex I and excluding, where applicable, commission and accrued interest.</p> <p>Where price is expressed in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the</p>	<p>{DECIMAL-18/13} in case the price is expressed in monetary value</p> <p>{DECIMAL-11/10} in case the price is expressed in percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is</p>

		<p>quantity of the quote currency for one unit of the base currency.</p> <p>This field shall be left blank in case of market orders.</p>	<p>expressed in basis points.</p>
6	Price currency	<p>Currency in which the trading price for the crypto-asset related to the order is expressed (applicable where the price is expressed as monetary value).</p> <p>Where the crypto-asset is traded in electronic money/e-money token, the identifier referred to in Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114] shall be used.</p> <p>Where price of the crypto-asset is expressed in monetary terms and it is expressed in a currency pair, the currency pair in which the price for the crypto-asset related to the order is expressed shall be reported. The first currency code shall be that of the base currency and the second currency code shall be that of the quote currency. The quote currency determines the price of one unit of the base currency. The ISO currency code and the DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI or alternative identifier referred to in Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to</p>	<p>To be populated in accordance with in Field 21 of Table 2 of Section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].</p>

		Article 68(10) of Regulation (EU) 2023/1114] shall be used to represent the fiat currency and the crypto asset respectively in the currency pair.	
7	Price notation	Indicates whether the price is expressed in monetary value, in percentage, in yield, in basis points.	<p>'MONE' — Monetary value</p> <p>'PERC' — Percentage</p> <p>'YIEL' — Yield</p> <p>'BAPO' — Basis points</p>
8	Quantity	<p>For crypto-assets traded in units, the number of units of the number of units of the crypto-asset.</p> <p>For crypto-assets not traded in units, the nominal or monetary value of the crypto-asset expressed in the same currency of the price in Field 5 "Price", as per Field 6 "Price currency".</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p> <p>Where Table 1 requires the aggregated publication of orders, the total number of units or the total nominal or monetary value of aggregated orders.</p>	<p>{DECIMAL-18/17} in case the quantity is expressed as number of units</p> <p>{DECIMAL-18/5} where the quantity is expressed as monetary or nominal value.</p>
9	Quantity currency	<p>Currency in which the quantity is expressed. The currency shall refer to the crypto-asset units, even when the transaction is denominated in sub-components of that crypto-asset.</p> <p>Field only needs to be populated where the quantity is expressed as a nominal monetary value or crypto-asset units.</p>	Identifier referred to in Field 26 of Table 2 of Section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of

			Regulation (EU) 2023/1114]
10	Quantity notation	Indicates whether the quantity reported is expressed in number of units, as a nominal value or as a monetary value, or crypto-asset units.	<p>— 'UNIT' — Number of units</p> <p>— 'NOML' — Nominal value</p> <p>— 'MONE' — Monetary value</p> <p>'{CRYP}' — Value in crypto-assets</p>
11	Venue	<p>Identification of the crypto-asset trading platform where the order was submitted.</p> <p>If the crypto-asset trading platform uses segment MICs then the segment MIC shall be used.</p> <p>If the crypto-asset trading platform does not use segment MICs then the operating MIC shall be used.</p>	{MIC}
12	Number of orders and quotes	The number of aggregated orders or quotes from different clients (where aggregated information is required under Table 1 of Annex I).	{DECIMAL-18/0}
13	Trading system	Type of trading system where the order or quote is advertised	<p>'CLOB' for continuous auction order book trading systems,</p> <p>'QDTS' for quote driven trading systems, 'PATS' for periodic auction trading systems,</p> <p>'HYBR' for hybrid trading systems,</p> <p>'AMMS' for automated market makers, 'XXXX' for any other trading</p>

			system
14	Publication date and time	Date and time when the information was published.	{DATE_TIME_FORMAT}

## ANNEX II

## Post-trade information to be made public

Table 1

## Symbol table

Symbol	Data type	Definition
{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{CURRENCYCODE_3}	3 alphanumerical characters	3-letter currency code, as defined by ISO 4217 currency codes
{DATE_TIME_FORMAT}	ISO 8601 date and time format	<p>Date and time in the following format: YYYY-MM-DDThh:mm:ss.dddZ.</p> <ul style="list-style-type: none"> <li>— 'YYYY' is the year;</li> <li>— 'MM' is the month;</li> <li>— 'DD' is the day;</li> <li>— 'T' — means that the letter 'T' shall be used</li> <li>— 'hh' is the hour;</li> <li>— 'mm' is the minute;</li> <li>— 'ss.ddd' is the second and its fraction of a second;</li> <li>— Z is UTC time.</li> </ul> <p>Dates and times shall be reported in UTC.</p>
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	<p>Numerical field for both positive and negative values.</p> <ul style="list-style-type: none"> <li>— decimal separator is '.' (full stop);</li> <li>— negative numbers are prefixed with '-' (minus);</li> </ul> <p>Where applicable, values shall be rounded and not truncated.</p>

{MIC}	4 alphanumerical characters	Market identifier as defined in ISO 10383
-------	-----------------------------	---

Table 2

**List of details for the purpose of post-trade transparency**

#	Field identifier	Content to be reported	Formats and standards to be used for reporting
1	Trading date and time	Date and time when the transaction was executed.	{DATE_TIME_FORMAT}
2	Crypto-asset identification code	Unique and unambiguous identifier of the crypto-asset in accordance with Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].	To be populated in accordance with Field 10 of table 2 of section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].
3	Crypto-asset full name	Full name of the crypto-asset.	{ALPHANUM-350}
4	Price	<p>Traded price of the transaction excluding, where applicable, commission, other fees and accrued interest.</p> <p>Where price recorded in monetary terms, it shall be provided in the major currency unit.</p> <p>— If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p>	{DECIMAL-18/13} where the price is expressed as a monetary value.
5	Missing Price	Where price is currently not available but pending, the value shall be 'PNDG'.	'PNDG' in case the price is not available



		Where price is not applicable, the value shall be 'NOAP'.	'NOAP' in case the price is not applicable
6	Price notation	Indicates whether the price is expressed in monetary value, in percentage, in yield, in basis points.	'MONE' – Monetary value  'PERC' – Percentage  'YIEL' – Yield  'BAPO' – Basis points
7	Price currency	<p>Currency in which the trading price for the crypto-asset related to the order is expressed (applicable where the price is expressed as monetary value).</p> <p>Where the crypto-asset is traded in electronic money/e-money token, the identifier referred to in Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114] shall be used.</p> <p>Where price of the crypto-asset is expressed in monetary terms and it is expressed in a currency pair, the currency pair in which the price for the crypto-asset related to the order is expressed shall be reported. The first currency code shall be that of the base currency and the second currency code shall be that of the quote currency. The quote currency determines the price of one unit of the base currency. The ISO currency code and the DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI or alternative identifier referred to in Article 15 of [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken</p>	<p>To be populated in accordance with in Field 21 of Table 2 of Section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114].</p>

		<p>pursuant to Article 68(10) of Regulation (EU) 2023/1114] shall be used to represent the fiat currency and the crypto asset respectively in the currency pair.</p>	
8	Quantity	<p>Field to be populated with the executed quantity.</p>	<p>{DECIMAL-18/17} in case the quantity is expressed as number of units</p> <p>{DECIMAL-18/5} where the quantity is expressed as monetary or nominal value.</p> <p>{DECIMAL-18/13} in case the price is expressed in sub-components of that crypto-asset</p>
9	Quantity currency	<p>Currency in which the quantity is expressed. The currency shall refer to the crypto-asset units, even when the transaction is denominated in sub-components of that crypto-asset.</p> <p>Field only needs to be populated where the quantity is expressed as a nominal monetary value or crypto-asset units.</p>	<p>Identifier referred to in Field 26 of Table 2 of Section 2 of the Annex to the [Delegated Regulation XX/XXXX specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken pursuant to Article 68(10) of Regulation (EU) 2023/1114]</p>
10	Quantity notation	<p>Indicates whether the quantity reported is expressed in number of units, as a nominal value or as a monetary value, or crypto-asset units.</p>	<ul style="list-style-type: none"> <li>— 'UNIT' — Number of units</li> <li>— 'NOML' — Nominal value</li> <li>— 'MONE' — Monetary value</li> <li>{CRYP} — Value in crypto-assets</li> </ul>

11	Venue of execution	<p>Identification of the crypto-asset trading platform where the order was submitted.</p> <p>If the crypto-asset trading platform uses segment MICs then the segment MIC shall be used.</p> <p>If the crypto-asset trading platform does not use segment MICs then the operating MIC shall be used.</p>	{MIC} – crypto-asset trading platform
12	Publication date and time	Date and time when the transaction was published by a crypto asset trading platform.	{DATE_TIME_FORMAT}
13	Venue of Publication	Code used to identify the crypto-asset trading platform publishing the transaction.	{MIC} – crypto-asset trading platform
14	Transaction identification code	Alphanumerical code assigned by crypto-asset trading platforms trading venues (pursuant to Article 12 of [Delegated Regulation (EU) xx/xxx on trade transparency, pursuant to Article 76(16)(b) of MiCA) used in any subsequent reference to the specific trade.	{ALPHANUM-52}

*Table 3*

**List of flags for the purpose of post-trade transparency**

<b>Flag</b>	<b>Name</b>	<b>Description</b>
'CANC'	Cancellation flag	When a previously published transaction is cancelled.
'AMND'	Amendment flag	When a previously published transaction is amended.

## 8.7 Annex VII: Draft RTS pursuant to Article 68(10)(b) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/...

of XXX

**supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken**

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 Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>74</sup>, and in particular Article 68(10), first subparagraph, point (b) thereof,

Whereas:

- (1) The records a crypto-asset service provider is required to keep should be adapted to the type of business and the range of crypto-asset services, activities, orders, and transactions undertaken by them, provided that the record-keeping obligations set out in Regulation (EU) 2023/1114, Regulation (EU) [*Delegated Regulation xx/xxx on RTS on complaints handling*], Regulation (EU) [*Delegated Regulation xx/xxx RTS on conflicts of interest*], Regulation (EU) 2023/1113 and this Regulation are fulfilled and that competent authorities are able to fulfil their supervisory tasks and take enforcement measures in view of ensuring both investor protection and market integrity.
- (2) Crypto-asset service providers should be free to determine the manner in which they keep records of relevant data relating to all orders and transactions in crypto-assets. However, consistent and comparable records on orders and transactions are essential for competent authorities to fulfil their supervisory tasks and to take enforcement measures. In particular, competent authorities should be able to seamlessly perform the same analysis on all record datasets, regardless of which crypto-asset service provider produced the record. Crypto-asset service providers should therefore provide consistent details of the records on orders and transactions by using uniform standards where a competent authority requests such information pursuant to Article 94 of Regulation (EU) 2023/1114.

---

<sup>74</sup>OJ L 150, 9.6.2023, p. 40.

- (3) In order to leverage from the knowledge and application of Regulation (EU) 600/2014 of the European Parliament and of the Council<sup>75</sup>, to ensure consistent reporting standards across financial sector and to minimise the reporting burden for crypto-asset service providers, certain data should be recorded in accordance with the standards referred to in the framework of that Regulation. In order to ensure consistency between this Delegated Regulation and the [*Delegated Regulation xx/xxx on order book records*], consistency and the same standards should apply when the records are also required in accordance with that Delegated Regulation.
- (4) Market abuse behaviours, including market manipulation, may be carried out through various means, including algorithmic trading. Therefore, in order to ensure effective market surveillance, where investment decisions are made by a person other than the client or by a computer algorithm, the person or algorithm should be identified in the order and transaction records using unique, robust and consistent identifiers. Where more than one person in a crypto-asset service provider makes the investment decision, the person taking the primary responsibility for the decision should be identified in the record.
- (5) In order to ensure unique, consistent and robust identification of natural persons referred to in order and transaction records, they should be identified by a concatenation of the country of their nationality followed by identifiers assigned by the country of nationality of those persons. Where those identifiers are not available, natural persons should be identified by identifiers created from a concatenation of their date of birth and name.
- (6) It is necessary that certain personal data are recorded by crypto-asset service providers to identify their clients or other natural persons relevant for orders or transactions in crypto-assets, as these data are fundamental to ensure efficient supervision by competent authorities, including in the area of market abuse. In compliance with the principle of data minimisation, such information should be necessary and sufficient to enable the competent authority to carry out a comprehensive assessment of the crypto-asset service provider's compliance with the relevant requirements of Regulation (EU) 2023/1114 and with market abuse provisions included in the same Regulation. When processing personal data included in the records, crypto-asset service providers and competent authorities should comply with the relevant provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>76</sup>.
- (7) In order to facilitate market surveillance and to allow comparability of the records, client identification should be reliable, open source, scalable, accessible, and unique across different crypto-asset service providers in accordance with the internationally established principles of the Financial Stability Board (FSB). In particular, the FSB recommends the

---

<sup>75</sup> Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

<sup>76</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

use of the unique international Legal Entity Identifier for an unambiguous and consistent identification of all parties to financial transactions. These include clients of Crypto Asset Service Providers that are legal entities. In contrast to national or regional codes or names of legal entities, LEI is a widely recognised, financially and operationally accessible international identifier. Only an international identifier that ensures access to the underlying data at all times allows for comparability and aggregation of information at the European level, improving the quality and timeliness of aggregated data and reducing the reporting burden for crypto-asset service providers. Furthermore, without a unique method for the identification and classification of parties and instruments that follow these principles any effort to achieve data-driven market monitoring by competent authorities cannot be achieved. Order and transaction records should therefore include the full name and date of birth of clients that are natural persons and should identify clients that are legal entities by their legal entity identifiers (LEIs). In light of the above, where the client does not have a LEI, the records should contain an identifier that ensures similar characteristics.

- (8) Manual or algorithmic abusive behaviours can occur also when determining the trading platform for crypto-asset to access or the crypto-asset service provider to which the orders are to be transmitted or any other conditions related to the execution of the order. Therefore, in order to ensure effective market surveillance, a person or computer algorithm within the crypto-asset service provider performing such activities should be identified in the order and transaction records. Where both a person and computer algorithm are involved, or more than one person or algorithm is involved, the crypto-asset service provider should determine, on a consistent basis following predetermined criteria, which person or algorithm is primarily responsible for those activities.
- (9) The details relating to the order to be transmitted between crypto asset service providers should be specified in order to ensure that the competent authorities have access to information that is relevant, accurate and complete.
- (10) Given the cross-border nature of crypto assets trading, in order to avoid data gaps where a crypto-asset service provider transmits orders or executes transactions via an entity that is not subject to Regulation (EU) 2023/1114, the records maintained by the crypto-asset service provider should cover the transmission or the execution, as if it was undertaken directly by the crypto-asset service provider, where such data is retrievable. Such information may be of particular importance for the performance of adequate market monitoring and market abuse supervision by the competent authority.
- (11) To properly monitor the integrity and stability of the markets in crypto-assets, competent authorities need reliable, consistent and standardised information on the crypto-assets that are traded. Such information should allow them to both identify the individual crypto-asset being traded and classify it according to internationally established principles. In addition, they should be able to retrieve the main characteristics of the crypto-assets, including their technology-specific features. Crypto-asset service providers should therefore use an internationally agreed digital token identifier to identify crypto-assets in



the order and transactions records that they provide to competent authorities. As identifier that is internationally agreed and guarantees reliable, consistent, standardised and available information, the Digital Token Identifier (DTI) should be used. Where it is not used, the crypto-asset service provider should record an equivalent unique identifier defined at Union level, meeting certain necessary characteristics including availability. In addition to DTI, the ISO code for the classification of financial instruments (CFI) is currently being revised to accommodate the classification of crypto-assets. Until the time such revision is finalised and the new CFI standard becomes available, an interim taxonomy indicating the type of crypto-assets as prescribed in this Regulation should be used.

- (12) In order to ensure efficient and effective market monitoring, transaction records should reflect whether the transaction was executed wholly or partly through a branch of the crypto-asset service provider located in another Member State or in a third country. The inclusion of granular data on branch activity in the records kept by the crypto-asset service providers, while not resulting in a disproportionate burden for the crypto-asset service provider, would allow competent authorities to more efficiently supervise the services provided by crypto-asset service providers and enhance the visibility on how the services are provided within territories of different Member States .
- (13) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (14) ESMA 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<sup>77</sup>,

HAS ADOPTED THIS REGULATION:

## *SECTION 1*

### **RETENTION OF RECORDS AND GENERAL PROVISION ON RECORDS**

#### *Article 1*

---

<sup>77</sup> 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).

## **Definitions**

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

- (1) “undertaking a transaction” means executing a transaction or transmitting an order;
- (2) “transaction” means the conclusion of an acquisition or disposal of a crypto-asset other than those crypto-assets referred to in Article 2(3) and (4) of Regulation (EU) 2023/1114;
- (3) “executing a transaction” means providing any of the following services or performing any of the following activities that result in a transaction:
  - (a) reception and transmission of orders in relation to one or more crypto-assets;
  - (b) execution of orders on behalf of clients;
  - (c) exchange of crypto-assets for funds or for other crypto-asset ;
  - (d) making an investment decision in accordance with a discretionary mandate given by a client;
  - (e) transfer of crypto-assets to or from accounts.

## *Article 2*

### **Retention of records**

1. The records shall be retained in a medium that allows the storage of information in a way accessible for future reference by the competent authority, and in such a form and manner that the following conditions are met:
  - (a) the competent authority is able to access them readily and to reconstitute each key stage of the processing of each service, activity, order or transaction;
  - (b) it is possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
  - (c) it is not possible for the records otherwise to be manipulated or altered;

- (d) it allows ICT or any other efficient exploitation when the analysis of the data cannot be easily carried out due to the volume and the nature of the data; and
  - (e) the firm's arrangements comply with the record keeping requirements irrespective of the technology used.
2. Crypto-assets service providers shall keep the records identified in the Annex, depending upon the nature of their services and activities.
  3. The list of records identified in the Annex is without prejudice to any other record-keeping obligations arising from other legislation.

## *SECTION 2*

### **Record keeping relating to specific crypto-asset services and to activities of crypto-asset service providers**

#### *Article 3*

##### **Record keeping of policies and procedures of the crypto-asset service provider**

1. Crypto-asset service providers shall keep records of any policies and procedures they are required to maintain pursuant to Regulation (EU) No 2023/1114 and their implementing measures in writing.
2. Crypto-asset service providers shall also keep an audit trail of the assessment and periodical review by the management body of the policy arrangements and policies and procedures put in place to comply with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114, including of any deficiencies identified in relation to such policy arrangements, policies and procedures and of any measures taken to address them.

#### *Article 4*

##### **Record keeping of rights and obligations of the crypto-asset service provider and the client**

1. Documents setting out the respective rights and obligations of the crypto-asset service provider and the client under an agreement to provide services, or the terms on which the crypto-asset service provider provides services to the client, shall be kept for a period of five years and, where requested by the competent authority before five years have elapsed,

for a period of up to seven years, from the date on which the agreement for the provision of services is terminated.

#### *Article 5*

#### **Record keeping in relation to the safekeeping of clients' crypto-assets and funds**

1. Crypto-asset service providers shall keep records enabling them at any time and without delay to distinguish crypto-assets and funds held for one client from crypto-assets and funds held for any other client and from their own assets.

Crypto-asset service providers shall maintain their records in a way that ensures that they may be used as an audit trail.

2. Such records shall include the following:
  - (a) records that readily identify the balances of crypto-assets and funds held for each client;
  - (b) where client funds are held by crypto-asset service providers in accordance with Article 70(2) and (3) of Regulation (EU) 2023/1114, details of the accounts in which client funds are held and on the relevant agreements with those credit institutions or central banks;
  - (c) details of the accounts opened with third parties holding crypto-assets for the crypto-assets service provider and of the outsourcing agreements with those third parties;
  - (d) details of third parties carrying out any tasks outsourced in accordance with Article 73 of Regulation (EU) 2023/1114 and details of the outsourced tasks;
  - (e) names and function of the staff of the crypto-asset service provider involved in the safekeeping of clients' crypto-assets and funds, including the staff responsible for the crypto-asset service provider's compliance with the requirements in relation to the safekeeping of clients' crypto-assets and funds;
  - (f) agreements relevant to establish client ownership over crypto-assets and funds.

### *SECTION 3*

## **Record keeping of orders and transactions**

### *Article 6*

#### **Record keeping of orders**

1. Crypto-asset service providers shall, in relation to every initial order received from a client and in relation to every initial decision to deal taken, to the extent they are applicable to the order or decision to deal in question, record and keep at the disposal of the competent authority the details set out in the second and third columns of Table 2 in Section 2 of the Annex and the details set out in the Table 4 in Section 4 of the Annex.
2. Where competent authorities request any of the details referred to in paragraph 1 in accordance with Article 94(1), points (a) or (d), and Article 94(3), point (a), of Regulation (EU) 2023/1114, the crypto-assets service providers shall provide such details as set out in the fourth column of Table 2 in Section 2 of the Annex.
3. Where the details set out in Table 2 in Section 2 of the Annex are also required pursuant to Article 76 of Regulation (EU) 2023/1114 or to Articles 25 and 26 of Regulation (EU) 600/2014, they shall be maintained in a consistent way and according to the same standards prescribed pursuant to Article 76 of Regulation (EU) 2023/1114 or to Articles 25 and 26 of Regulation (EU) 600/2014.

### *Article 7*

#### **Record keeping of transactions**

1. Crypto-asset service providers shall, immediately after undertaking a transaction, record and keep at the disposal of the competent authority the details set out in the second and third columns of the Tables in Section 3 and 4 of the Annex.
2. Where competent authorities request any of the details referred to in paragraph 1 in accordance with Article 94(1), points (a) or (d), and Article 94(3), point (a), of Regulation (EU) 2023/1114, the operators of trading platforms for crypto-assets shall provide such details as set out in the fourth column of the Table 3 in Section 3 of the Annex.

### *Article 8*

#### **Identification of person or computer algorithm within the crypto-asset service provider making the investment decision**

1. Where a person or computer algorithm within a crypto-asset service provider makes the investment decision to acquire or dispose of a specific crypto-asset on behalf of the crypto-asset service provider or on behalf of a client in accordance with a discretionary mandate given by the client, that person or computer algorithm shall be identified and recorded as specified in Field 41 of the Table 3 in Section 3 of the Annex.
2. Where a person and computer algorithm are both involved in taking the investment decision, or more than one person or algorithm are involved, the crypto-asset service provider shall record which person or computer algorithm is primarily responsible for that decision.

#### *Article 9*

#### **Designation to identify natural persons**

1. A client that is a natural person shall be identified in the crypto-asset service provider records using the designation resulting from the concatenation of the ISO 3166-1 alpha-2 (2 letter country code) of the nationality of the person, followed by the national client identifier specified in Annex II of Delegated Regulation (EU) 2017/590<sup>78</sup>, based on the nationality of the person.
2. The national client identifier referred to in paragraph 1 shall be assigned in accordance with the priority levels provided in Annex II of Delegated Regulation (EU) (EU) 2017/590 using the highest priority identifier that a person has regardless of whether that identifier is already known to the crypto-asset service provider.
3. Where a natural person is a national of more than one European Economic Area (EEA) country, the country code of the first nationality when sorted alphabetically by its ISO 3166-1 alpha-2 code and the identifier of that nationality assigned in accordance with paragraph 2 shall be used. Where a natural person has a non-EEA nationality, the highest priority identifier in accordance with the field referring to 'all other countries' provided in Annex II of Delegated Regulation (EU) 2017/590 shall be used. Where a natural person has EEA and non-EEA nationality, the country code of the EEA nationality and the highest priority identifier of that nationality assigned in accordance with paragraph 2 shall be used.
4. Where a client is a resident of a country other than the one of its nationality, crypto-asset service providers shall also identify natural persons based on the country of residence of the person in the same manner as described in paragraphs 1 to 3.

---

<sup>78</sup> Delegated Regulation (EU) 2017/590 of 28 July 2016, supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities (OJ L 87, 31.3.2017, p. 449).

5. Where the identifier assigned in accordance with paragraph 2 is based on CONCAT, the natural person shall be identified by the crypto-asset service provider using the concatenation of the following elements in the following order:
  - (a) the date of birth of the person in the format YYYYMMDD;
  - (b) the five first characters of the first name;
  - (c) the five first characters of the surname.
6. For the purposes of paragraph 5, prefixes to names shall be excluded and first names and surnames shorter than five characters shall be appended by '#' so as to ensure that references to names and surnames in accordance with paragraph 4 contain five characters. All characters shall be in upper case. No apostrophes, accents, hyphens, punctuation marks or spaces shall be used.

#### *Article 10*

##### **Identification of person or computer algorithm determining conditions for the execution of a transaction**

1. Where a person or computer algorithm within the crypto-asset service provider which executes a transaction determines which trading platform for crypto-assets located outside the Union to access, which other crypto-asset service provider to transmit orders to or any conditions related to the execution of a transaction, that person or computer algorithm shall be identified in Field 41 of the Table 3 in Section 3, of the Annex.
2. Where a person within the crypto-asset service provider takes decisions determining the execution of the transaction, the crypto-asset service provider shall assign a designation for identifying that person in its transaction records in accordance with Article 9.
3. Where a computer algorithm within the crypto-asset service provider takes decisions determining the execution of the transaction, that computer algorithm shall be identified in Field 43 of the Table 3 in Section 3 of the Annex.
4. Where a person and computer algorithm are both involved in execution of the transaction, or more than one person or algorithm are involved, the crypto-asset service provider shall record which person or computer algorithm is primarily responsible for the execution of the transaction.

#### *Article 11*

##### **Reception and transmission of an order**



1. Crypto-asset service providers receiving and transmitting an order to another crypto-asset service provider in accordance with Article 1(3)(a), shall record the order details as described in Fields 1, 2, 10, 12, 14, 15, 16, 17, 19, 20, 21, 25, 37 of Table 2 in Section 2 of the Annex, insofar as pertinent to a given order.
2. Where the order transmitted was received from a prior transmitting crypto-asset service provider, the code provided pursuant to the first subparagraph shall be the code identifying the prior transmitting crypto-asset service provider.
3. Where the order is transmitted more than one time, the order details referred to in paragraph 1, shall be recorded in respect of the client of the first transmitting crypto-asset service provider.
4. Where orders are aggregated for more than one client, information referred to in paragraph 1 shall be recorded for each client.

#### *Article 12*

#### **Recording of orders and transactions executed via entities not subject to Regulation (EU) 2023/1114**

1. Where a crypto-asset service provider provides the service of execution of orders through a trading platform for crypto-assets or a service provider that is not subject to Regulation (EU) 2023/1114, the crypto-asset service provider shall record the details of the order as if the execution was undertaken by the crypto-asset service provider.
2. The crypto-asset service provider shall record the information referred to in the first paragraph as set out in Table 2 in Section 2, and in the Table 3 in Section 3 of the Annex to the extent they are retrievable for the order or transaction in question.

#### *Article 13*

#### **Recording of reception and transmission of orders to entities not subject to Regulation (EU) 2023/1114**

1. Where a crypto-asset service provider transmits an order to a firm that is not subject to Regulation (EU) 2023/1114, the crypto-asset service provider shall record the details of the transmitted order as set out in Table 2 in Section 2 of the Annex insofar as pertinent to the order and to the extent that they are retrievable.

2. Where the order is aggregated for several clients, the information referred to in Article 9 and 14, as applicable, shall be recorded for each client.

#### *Article 14*

##### **Identification of clients that are legal entities**

1. When providing information to competent authorities as referred to in Articles 6 and 7, a crypto-asset service provider shall identify clients that are legal entities by using the legal entity identifier provided by that client.
2. The crypto-asset service provider shall record legal entity identifier codes compliant with the ISO 17442 standard and included in the Global LEI database maintained by the Central Operating Unit appointed by the Regulatory Oversight Committee and pertaining to the entity concerned.
3. Where the client does not have a legal entity identifier compliant with the ISO 17442 standard, the crypto asset service provider shall obtain the ISO 17442 for the client or use an identifier defined at Union level which meets all of the following characteristics:
  - (a) is unique;
  - (b) is neutral;
  - (c) is reliable;
  - (d) is open source;
  - (e) is scalable;
  - (f) is accessible;
  - (g) is available at a reasonable cost, and
  - (h) is subject to an appropriate governance framework.

#### *Article 15*

##### **Identification of crypto assets**

1. When providing information to competent authorities under Articles 6 and 7, a crypto-asset service provider shall identify the crypto-assets that are object of the recorded order or

transaction, or used as a means of payment, by using a digital token identifier that is compliant with the ISO 24165 standard or an equivalent unique identifier defined at Union level, which meets all of the following characteristics:

- (a) is unique;
- (b) is neutral;
- (c) is reliable;
- (d) is open source;
- (e) is scalable;
- (f) is accessible;
- (g) is available at a reasonable cost basis, and
- (h) is subject to an appropriate governance framework.

#### *Article 16*

#### **Recording of transactions undertaken by branches**

1. Where a crypto-asset service provider undertakes a transaction wholly or partly through its branch, it shall include in its transaction records the ISO 3166 country code of such branch, in accordance with Fields 7, 16, 34, 42 or 44 of Table 3 in Section 3 of the Annex.
2. Where applicable the crypto-asset service provider shall include in the record the indication of the following information:
  - (a) whether the branch received the order from a client or made an investment decision for a client in accordance with a discretionary mandate given to it by the client;
  - (b) whether the branch has supervisory responsibility for the person taking the investment decision concerned;
  - (c) whether the branch has supervisory responsibility for the person determining the conditions for execution of the transaction;
  - (d) whether the transaction was fully or partially undertaken on a trading platform for crypto-asset located outside the Union using the branch's membership of that trading platform for crypto-assets.

*Article 17*

**Identification of the crypto-asset service provider undertaking orders and transactions**

1. A crypto-asset service provider which undertakes orders or transactions triggering the obligation to keep records shall ensure that it is identified in the records to be maintained pursuant to this Regulation with a legal entity identifier compliant with the ISO 17442 standard and included in the Global LEI database maintained by the Central Operating Unit appointed by the Regulatory Oversight Committee and pertain to the entity concerned.
2. The crypto-asset service provider shall ensure that the reference data related to its legal entity identifier is renewed in accordance with the terms of any of the accredited Local Operating Units of the Global Legal Entity Identifier System.

*Article 18*

**Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission  
The President

[For the Commission  
On behalf of the President

[Position]

*ANNEX*

*SECTION 1*

**Records of services and activities: list of records to be kept by crypto-asset service providers depending upon the nature of their services and activities**

Type of record	Summary of content
<b>Communication with clients</b>	
Marketing communications	Each marketing communication issued by the crypto-asset service provider (except in oral form) or on its behalf.
Information to clients	Information other than marketing communication provided by the crypto-asset service provider, or on its behalf, to the client with regard to the crypto-asset service provider, its services and activities, crypto-assets as well as the applicable costs and related charges.
Records of communication with clients	Records of telephone conversations or electronic communications relating to transactions or to the reception, transmission and execution of client orders, including where such conversations or communications do not result in the conclusion of a transaction or in the provision of the services of reception and transmission of orders or execution of order.
<b>Rights and obligations of the crypto-asset service provider and the client</b>	
Client agreements	The document or documents agreed between the crypto-asset service provider and the client that set out the rights and obligations of the parties.

Consent of the client	Any communication between the crypto-asset service provider and the client or any document evidencing that the client consented to the provision of services and to the terms on which the crypto-asset service provider will provide such services to the client.
<b>Market abuse</b>	
Market abuse	Records of instances where circumstances indicate that market abuse has been committed, is being committed or is likely to be committed. Such records shall include, at least, the identification of the relevant persons or computer algorithms. For persons professionally arranging or executing transactions in crypto-assets, the records shall include the information referred to in Article [3(5)] of [ <i>Delegated Regulation (EU) xx/xxx RTS on STORs pursuant to Article 92 of MiCA</i> ]
<b>Safekeeping of clients' crypto-assets and funds</b>	
Clients' crypto-assets and means of access to crypto-assets held by the crypto-asset service provider	The records enabling the crypto-asset service provider to safeguard the ownership rights of clients and to prevent the use of clients' crypto-assets for their own account, in accordance with Article 70(1) of Regulation (EU) No 2023/1114.
Clients' funds held by a crypto-asset service provider	The records enabling the crypto-asset service provider to safeguard the ownership rights of clients and to prevent the use of clients' funds for their own account in accordance with Article 70(2) of Regulation (EU) No 2023/1114. Any document, records or evidence showing that the crypto-asset service provider complies with its obligations under Article 70(3) of Regulation (EU) No 2023/1114.
<b>Complaints handling</b>	
Complaints	The records as provided in Article [XX] of [ <i>Commission Delegated Regulation (EU) xx/xxx on RTS on complaints handling</i> ].

<b>Conflicts of interest and personal transactions</b>	
Conflicts of interest	The records as provided in Article [XX] of [ <i>Commission Delegated Regulation (EU) xx/xxx on RTS on conflicts of interest</i> ].
Personal transaction	The records as provided in Article [XX] of [ <i>Commission Delegated Regulation (EU) xx/xxx on RTS on conflicts of interest</i> ].
<b>Outsourcing</b>	
Outsourcing agreements	Records of the written agreements as provided in Article 73(3) of Regulation (EU) 2023/1114.
Outsourced services and activities	Records of any service or activity outsourced to a third party together with, at least: <ul style="list-style-type: none"> <li>(a) the name, registered office, operating address and regulatory status of the third party to which the service or activity, or any part of the service or activity, was outsourced;</li> <li>(b) the name, function and contact details of the person in charge of the service or activity, or part of the service or activity, at the third party to which the service or activity, or any part of the service or activity, was outsourced;</li> <li>(c) the name and function of the person in charge of the service or activity, or part of the service or activity, at the crypto-asset service provider.</li> </ul>
<b>Custody and administration of crypto-assets on behalf of clients</b>	
Register of positions	Records of the registers of positions as provided in Article 75(2) and (4) of Regulation (EU) 2023/1114.
Statement of positions	Records of the statement of positions, as provided in Article 75(5) of Regulation 2023/1114.
Communications with clients	Records of any communication with the client as provided in Article 75(5), second subparagraph, of Regulation 2023/1114 including the response received by the client or lack thereof.



Use of other crypto-asset service providers	<p>Where clients' crypto-assets or means of access to crypto-assets are safekept or controlled in accordance with Article 75(9) of Regulation (EU) 2023/1114:</p> <p>a) records from the third party crypto-asset service provider evidencing the positions of the clients;</p> <p>b) records of communications evidencing that the crypto-asset service provider complied with Article 75(9), second subparagraph of Regulation (EU) 2023/1114.</p>
<b>Operation of a trading platform for crypto-assets</b>	
Operating rules	A copy of the operating rules provided in Article 76(1) of Regulation (EU) 2023/1114, including deficiencies detected and the measures taken to remedy them.
Assessment of suitability of the crypto-asset	Records of the assessment conducted pursuant to Article 76(2) of Regulation (EU) 2023/1114 and its outcome.
In-built anonymisation function	Records of cases where crypto-assets have an in-built anonymisation function.
Consent of the client to matched principal trading	Records of clients' consent to the crypto-asset service provider engaging in matched principal trading on the platform for crypto-assets that it operates, as provided in Article 76(6) of Regulation (EU) 2023/1114.
<b>Exchange of crypto-assets for funds or other crypto-assets</b>	
Price and limits	<p>Records of the price of the crypto-assets or of the method for determining the price of the crypto-assets proposed to exchange for funds or other crypto-assets, as well as any applicable limits determined by the crypto-asset service provider on the amount to be exchanged, as provided in Article 77(2) of Regulation (EU) 2023/1114.</p> <p>Such records shall include for each price, method for determining the price and applicable limit:</p> <ul style="list-style-type: none"> <li>- the identification of the crypto-asset;</li> <li>- If the crypto-asset can be exchanged for funds or crypto-assets or both;</li> </ul>

	<ul style="list-style-type: none"> <li>- The price of the crypto-asset;</li> <li>- The amount of crypto-assets you an exchange another crypto-asset for.</li> </ul>
<b>Placing of crypto-assets</b>	
Information to clients or prospective clients	Records of the communications made in accordance with Article 79(1) of Regulation (EU) 2023/1114 and of the consent received from the offeror or person seeking admission to trading or any third party acting on its behalf.
Placing operations	Records of any placing operation of the crypto-asset service provider, as provided in Article [XX] of [ <i>Commission Delegated Regulation (EU) xx/xxx on RTS on conflicts of interest</i> ].
<b>Advice and portfolio management</b>	
Information to clients	Records of any communication made in accordance with Article 81(2), (4) and (9) of Regulation (EU) 2023/1114.
Assessment of suitability	<p>Records of all information collected from each client and assessed to conduct the suitability assessment referred to in paragraph 1 of Article 81 of Regulation (EU) 2023/1114, as well as all internal documents relating to such suitability assessment.</p> <p>Records of clients who did not provide the information required pursuant to Article 81(8) of Regulation (EU) 2023/1114.</p>
Investment advice	Records of the time and date on which advice on crypto-assets was rendered, records of the crypto-assets that were recommended and the suitability report provided to the client in accordance with Article 81(13) of Regulation (EU) 2023/1114.
Periodic statement for portfolio management services	Records of any periodic statement provided to the client in accordance with Article 81(14) of Regulation (EU) 2023/1114.

<p>Inducements</p>	<p>1. Records of any minor non-monetary benefit received by the crypto-asset service provider in accordance with Article 81(3), second subparagraph, of Regulation (EU) 2023/1114. Such records shall include, at least:</p> <ul style="list-style-type: none"> <li>(a) the nature of the minor non-monetary benefit and the date it was received;</li> <li>(b) the client and service or activity in relation to which it was received;</li> <li>(c) how such minor non-monetary benefit complies with Article 81(3), second subparagraph, of Regulation (EU) 2023/114.</li> </ul> <p>2. Records of any inducements received by the crypto-asset service provider in accordance with Article 81(6) of Regulation (EU) 2023/1114. Such records shall include, at least:</p> <ul style="list-style-type: none"> <li>(a) the nature, amount and date the inducement was received;</li> <li>(b) the client and service or activity in relation to which it was received;</li> <li>(c) how such inducement complies with Article 81(6), first subparagraph, of Regulation (EU) 2023/114;</li> <li>(d) any communication made in accordance with Article 81(6), second subparagraph, of Regulation (EU) 2023/1114.</li> </ul>
<p><b>Transfer services</b></p>	
<p>Records to be kept by the crypto-asset service provider of the originator</p>	<p>Records of:</p> <ul style="list-style-type: none"> <li>(a) all instructions received; and</li> <li>(b) all information listed in Article 14(1) to (3) of Regulation (EU) 2023/1113;</li> <li>(c) the means of verification as provided in Article 14(6) of Regulation (EU) 2023/1113;</li> <li>(d) any suspension or rejection of any instruction to carry out a transfer of crypto-asset and the reason for such suspension or rejection.</li> </ul>

Records to be kept by the crypto-asset service provider of the beneficiary	Records of: (a) all information listed in Article 14(1) to (3) of regulation (EU) 2023/1113; (b) the means of verification as provided for in Article 16(3) of Regulation 2023/1113; (c) any return, suspension or rejection of a transfer of crypto-asset and the reason for such return, suspension or rejection; (d) any measures taken in accordance with Article 17(2) of Regulation (EU) 2023/1113, together with the identification of the relevant crypto-asset service providers.
Records to be kept by intermediary crypto-asset service providers	Records of: (a) all information listed in Article 14(1) to (3) of regulation (EU) 2023/1113; (b) any return, suspension or rejection of a transfer of crypto-asset and the reason for such return, suspension or rejection; (c) any measures taken in accordance with Article 21(2) of Regulation (EU) 2023/1113, together with the identification of the relevant crypto-asset service providers.

*SECTION 2*

**Records of orders**

*Table 1*

**Legend for Table 2 of Section 2 and for Section 3**

Symbol	Data type	Definition
--------	-----------	------------

{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{CFI_CODE}	6 characters	ISO 10962 CFI code
{COUNTRYCODE_2}	2 alphanumerical characters	2 letter country code, as defined by ISO 3166-1 alpha-2 country code
{CURRENCYCODE_3}	3 alphanumerical characters	3 letter currency code, as defined by ISO 4217 currency codes
{DATE_TIME_FORMAT}	ISO 8601 date and time format	<p>Date and time in the following format:          YYYY-MM-DDThh:mm:ss.dxxxxxZ.</p> <ul style="list-style-type: none"> <li>– ‘YYYY’ is the year;</li> <li>– ‘MM’ is the month;</li> <li>– ‘DD’ is the day;</li> <li>– ‘T’ – means that the letter ‘T’ shall be used</li> <li>– ‘hh’ is the hour;</li> <li>– ‘mm’ is the minute;</li> <li>– ‘ss.dxxxxx’ is the second and its fraction of a second;</li> <li>– Z is UTC time.</li> </ul> <p>Dates and times shall be recorded in UTC.</p>
{DATEFORMAT}	ISO 8601 date format	Dates shall be formatted in the following format: YYYY-MM-DD.

{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	Numerical field for both positive and negative values. – decimal separator is ‘.’ (full stop); – negative numbers are prefixed with ‘-’ (minus); Values are rounded and not truncated.
{DTI}	9 alphanumerical characters	Digital token identifier as defined in ISO 24165 standard
{DTI_SHORT_NAME }	n alphanumeric characters	DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI
{INTEGER-n}	Integer number of up to n digits in total	Numerical field for both positive and negative integer values.
{ISIN}	12 alphanumerical characters	ISIN code, as defined in ISO 6166
{LEI}	20 alphanumerical characters	Legal entity identifier as defined in ISO 17442

{MIC}	4 alphanumeric characters	Market identifier as defined in ISO 10383
{NATIONAL_ID}	35 alphanumeric characters	The identifier is derived in accordance with Article 9 and Annex II of Commission Delegated Regulation (EU) 2017/590

*Table 2*

**Details of orders to be kept**

<b>Field Number</b>	<b>Field Name</b>	<b>Field description</b>	<b><i>Details on the order data to be provided to the competent authority</i></b>
Section A — Identification of the relevant parties			
1	Client identification code	<p>Code used to identify the client of the crypto-assets service provider which submitted the order.</p> <p>Where the client is a legal entity, the LEI code of the client or the alternative identifier referred to in Article 14.3 shall be used.</p> <p>Where the client is not a legal entity, the {NATIONAL_ID} shall be used.</p> <p>In case of pending allocations, the flag PNAL shall be used.</p>	{LEI} {NATIONAL_ID} {ALPHANUM-20} {PNAL} 'NOAP'



		This field shall be 'NOAP' where the crypto-asset service provider has a direct interest to buy or sell.	
2	Investment decision within the CASP	<p>Code used to identify the person or the algorithm within the crypto assets service provider who is taking the investment decision.</p> <p>Where a natural person within the crypto-asset service provider takes the investment decision the person who is responsible or has primary responsibility for the investment decision shall be identified with the {NATIONAL_ID}</p> <p>Where an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity took the investment decision the field shall be populated with a code assigned according to Article 8.</p> <p>This field shall be left blank when the investment decision was not made by a person or algorithm within the crypto asset service provider.</p>	<p>{NATIONAL_ID} — Natural persons</p> <p>{ALPHANUM-50} — Algorithms</p>
3	Execution within firm	<p>Code used to identify the person or algorithm within the crypto-asset service provider determining the conditions for the execution of the transaction resulting from the order.</p> <p>Where a natural person determines the execution of the transaction, the person shall be identified by {NATIONAL_ID}</p> <p>Where an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity is responsible for the execution of the transaction, this field shall be populated with a code assigned by the crypto asset service provider, in accordance with Article 10.</p> <p>Where more than one person or a combination of persons and algorithms are involved in the execution of the transaction, the crypto asset service provider shall determine the trader or algorithm primarily responsible and populate this field with the identity of that trader or algorithm</p>	<p>{NATIONAL_ID} — Natural persons</p> <p>{ALPHANUM-50} — Algorithms</p>
Section B — Trading capacity and liquidity provision			

4	Trading capacity	<p>Indicates whether the crypto-asset service provider undertaking the transaction is carrying out matched principal trading, as defined under Article 3(1), point 40 of Regulation (EU) 2023/1114 or exchange crypto-assets for funds as defined under Article 3(1), point 19 of Regulation (EU) 2023/1114.</p> <p>Where the order submission does not result from the crypto-asset service provider carrying out matched principal trading or exchanging crypto-assets for funds or other crypto-assets, the field shall indicate that the transaction was carried out under any other capacity.</p>	<p>'DEAL' — Exchange crypto-assets for funds or other crypto-assets</p> <p>'MTCH' — Matched principal</p> <p>'AOTC' — Any other capacity</p>
Section C — Date and time			
5	Date and Time	The date and time for each event listed in Section [G] and [J].	{DATE_TIME_FORMAT}
Section D — Validity period and order restrictions			
6	Validity period	<p>Good-For-Day: the order expires at the end of the trading day on which it was entered in the order book</p> <p>Good-Till-Cancelled: the order will remain active in the order book and be executable until it is actually cancelled.</p> <p>Good-Till-Time: the order expires at the latest at a pre-determined time within the current trading session.</p> <p>Good-Till-Date: the order expires at the end of a specified date.</p> <p>Good-Till-Specified Date and Time: the order expires at a specified date and time.</p> <p>Good After Time: the order is only active after a pre-determined time within the current trading session.</p> <p>Good After Date: the order is only active from the beginning of a pre-determined date</p>	<p>'DAVY' — Good-For-Day</p> <p>'GTCV' — Good-Till-Cancelled</p> <p>'GTTV' — Good-Till-Time</p> <p>'GTDV' — Good-Till-Date</p> <p>'GTSV' — Good-Till-Specified Date and Time</p> <p>'GATV' — Good After Time</p>

		<p>Good After Specified Date and Time: the order is only active from a pre-determined time on a pre-determined date.</p> <p>Immediate-Or-Cancel: an order which is executed upon its entering into the order book (for the quantity that can be executed) and which does not remain in the order book for the remaining quantity (if any) that has not been executed.</p> <p>Fill-Or-Kill: an order which is executed upon its entering into the order book provided that it can be fully filled: in the event the order can only be partially executed, then it is automatically rejected and cannot therefore be executed.</p> <p>Other: any additional indications that are unique for specific business models, trading platforms or systems.</p>	<p>‘GADV’ — Good After Date</p> <p>‘GASV’ — Good After Specified Date and Time</p> <p>‘IOCV’ — Immediate-Or-Cancel</p> <p>‘FOKV’ — Fill-Or-Kill</p> <p>or</p> <p>{ALPHANUM-4} character’ not already in use for the trading venue's own classification.</p>
7	Order restriction	<p>Good For Closing Price Crossing Session: where an order qualifies for the closing price crossing session.</p> <p>Valid For Auction: the order is only active and can only be executed at auction phases (which can be pre-defined by the CASP client who submitted the order, e.g. opening and/closing auctions and/or intraday auction).</p> <p>Valid For Continuous Trading only: the order is only active during continuous trading.</p> <p>Other: any additional indications that are unique for specific business models, trading platforms or systems.</p>	<p>‘SESR’ — Good For Closing Price Crossing Session</p> <p>VFAR’ — Valid For Auction</p> <p>‘VFCR’ — Valid For Continuous Trading only</p> <p>{ALPHANUM-4} character’ not already in</p>

			<p>use for the trading venue's own classification.</p> <p>This field shall be populated with multiple flags separated by a comma where more than one flag is applicable</p>
8	Validity period and time	<p>This field refers to the time stamp reflecting the time on which the order becomes active or it is ultimately removed from the order book:</p> <p>Good for day: the date of entry with the timestamp immediately prior to midnight</p> <p>Good till time: the date of entry and the time to that specified in the order</p> <p>Good till date: will be the specified date of expiry with the timestamp immediately prior to midnight</p> <p>Good till specified date and time: the specified date and time of expiry</p> <p>Good after time: the date of entry and the specified time at which the order becomes active</p> <p>Good after date: the specified date with the timestamp immediately after midnight</p> <p>Good after specified date and time: the specified date and time at which the order becomes active</p>	{DATE_TIME_FORMAT}

		<p>Good till Cancel: the ultimate date and time the order is automatically removed by market operations</p> <p>Other: timestamp for any additional validity type.</p>	
Section E — Identification of the order			
9	Segment MIC code	<p>Identification of the trading platform for crypto-asset where the order was submitted.</p> <p>If the trading platform for crypto-asset uses segment MICs then the segment MIC shall be used.</p> <p>If the trading platform for crypto-asset does not use segment MICs then the operating MIC shall be used.</p> <p>This field shall only be populated for orders to be executed on a trading platform for crypto-asset.</p>	{MIC}
10	Crypto-asset identification code	Unique and unambiguous identifier of the crypto-asset	{DTI} {ALPHANUM-20}
11	Crypto-asset classification	<p>Taxonomy used to classify the crypto-asset.</p> <p>or</p> <p>A complete and accurate CFI code shall be provided when available.</p>	ART EMT OT  {CFI_CODE}
12	Order identification code	An alphanumeric code assigned by the operator of the trading platform for crypto-assets to the individual order.	{ALPHANUM-50}

Section F — Events affecting the order			
13	New order, order cancellation	<p>New order: submission of a new order to the CASP operating the trading platform for crypto-assets.</p> <p>Cancelled at the initiative of the client of the CASP: where the client decides upon its own initiative to cancel the order it has previously entered.</p>	<p>‘NEWO’ — New order</p> <p>‘CAME’ — Cancelled at the initiative of the client of the CASP</p> <p>.</p>
Section G — Type of order			
14	Order type	Identifies the type of order submitted to the trading platform for crypto-asset as per the trading platform for crypto-asset specifications.	{ALPHANUM-50}
15	Order type classification	<p>Classification of the order according to two generic order types. LIMIT order: in the cases where the order is tradable and</p> <p>STOP order: in the cases where the order becomes tradable only upon the realisation of a pre-determined price event.</p>	The letters ‘LMTO’ for limit or the letters ‘STOP’ for stop.
Section H — Prices			
16	Limit price	<p>The maximum price at which a buy order can trade or the minimum price at which a sell order can trade.</p> <p>The spread price for a strategy order. It can be negative or positive.</p> <p>This field shall be ‘NOAP’ in case of orders that do not have a limit price or in case of unpriced orders.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p>	<p>{DECIMAL-18/13} in case the price is expressed as monetary value.</p> <p>{DECIMAL-11/10} in case the price is</p>

		<p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
17	Additional limit Price	<p>Any other limit price which may apply to the order. This field shall be left 'NOAP' if not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10 where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
18	Stop price	<p>The price that must be reached for the order to become `active.</p> <p>For stop orders triggered by events independent of the price of the crypto-asset, this field shall be populated with a stop price equal to zero.</p> <p>This field shall be 'NOAP' if not relevant.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p>



		<p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-11/10 where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
19	Pegged limit price	<p>The maximum price at which a pegged order to buy can trade or the minimum price at which a pegged order to sell can trade.</p> <p>This field shall be 'NOAP' if not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10 where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
20	Transaction price	<p>Traded price of the transaction excluding, where applicable, commission, other fees and accrued interest.</p> <p>Where price recorded in monetary terms, it shall be provided in the major currency unit.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p>

		<p>Where price is not applicable the field shall be populated with the value 'NOAP'.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p>	'NOAP'
21	Price currency	<p>Currency in which the trading price for the crypto-asset related to the order is expressed (applicable where the price is expressed as monetary value).</p> <p>Where the crypto-asset is traded in electronic money/e-money token, the Digital Token Identifier or the alternative identifier referred to in Article 15 shall be used.</p> <p>Where price of the crypto-asset is expressed in monetary terms and it is expressed in a currency pair, the currency pair in which the price for the crypto-asset related to the order is expressed shall be reported. The first currency code shall be that of the base currency and the second currency code shall be that of the quote currency. The quote currency determines the price of one unit of the base currency. The ISO currency code and the DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI or alternative identifier shall be used to represent the fiat currency and the crypto asset respectively in the currency pair.</p>	<p>{CURRENCYCODE_3}</p> <p>{DTI}</p> <p>{ALPHANUM-20}</p> <p>{CURRENCYCODE_3} should be used for fiat currencies in a currency pair</p> <p>{DTI_SHORT_NAME} should be used for crypto assets in a currency pair</p> <p>'NOAP'</p>
22	Price notation	Indicates whether the price is expressed in monetary value, in percentage, in yield or in basis points.	<p>'MONE' — Monetary value</p> <p>'PERC' — Percentage</p> <p>'YIEL' — Yield</p> <p>'BAPO' — Basis points</p>
Section I — Order instructions			
23	Buy-sell indicator	To show if the order is to buy or sell.	'BUYI' — buy

			'SELL' — sell
24	Order status	To identify orders that are active/inactive/suspended: Active — non-quote orders that are tradable. Inactive — non-quote orders that are not tradable.	'ACTI'- active or 'INAC'- inactive
25	Quantity notation	Indicates whether the quantity reported is expressed in number of units, as a nominal value or as a monetary value, or crypto-assets units.	'UNIT' — Number of units 'NOML' — Nominal value 'MONE' — Monetary value 'CRYP' – Crypto-asset
26	Quantity currency	Currency in which the quantity is expressed. The currency shall refer to the crypto-asset units, even when the transaction is denominated in sub-components of that crypto-asset. Field only needs to be populated where the quantity is expressed as a nominal or monetary value or crypto-assets units.	{CURRENCYCODE_3} {DTI} {ALPHANUM-20}
27	Initial quantity	The number of units of the crypto-asset in the order. In case the order pertains a fraction of a crypto-asset, indicate the quantity in decimal notation of the unit. The nominal or monetary value of the crypto-asset.	{DECIMAL-18/17} in case the quantity is expressed as number of units

			{DECIMAL-18/5} in case the quantity is expressed as monetary or nominal value
28	Remaining quantity	<p>The total quantity that remains in the order book after a partial execution or in the case of any other event affecting the order.</p> <p>On a partial fill order event, this shall be the total remaining volume after that partial execution. On an order entry this shall equal the initial quantity.</p>	<p>{DECIMAL-18/17} in case the quantity is expressed as a number of units</p> <p>{DECIMAL-18/5} where the quantity is expressed as monetary or nominal value</p>
29	Traded quantity	Where there is a partial or full execution, this field shall be populated with the executed quantity	<p>{DECIMAL-18/17} in case the quantity is expressed as a number of units</p> <p>{DECIMAL-18/5} where the quantity is expressed as monetary or nominal value</p>

30	Minimum Acceptable Quantity (MAQ)	The minimum acceptable quantity for an order to be filled which can consist of multiple partial executions and is normally only for non-persistent order types. This field shall be 'NOAP' if not relevant.	{DECIMAL-18/17} in case the quantity is expressed as a number of units {DECIMAL-18/5} where the quantity is expressed as monetary or nominal value 'NOAP'
31	Minimum executable size (MES)	The minimum execution size of any individual potential execution. This field shall be left blank if not relevant.	{DECIMAL-18/17} in case the quantity is expressed as a number of units {DECIMAL-18/5} where the quantity is expressed as monetary or nominal value
32	MES first execution only	Specifies whether the MES is relevant only for the first execution. This field can be left blank where field 29 is left blank.	'true' 'false'

33	Passive only indicator	Indicates if the order is submitted to the trading platform for crypto-asset with a characteristic/flag, such that the order shall not immediately execute against any contra visible orders.	'true' 'false'
34	Passive or aggressive indicator	On partial fill and fill order events, indicates whether the order was already resting on the order book and providing liquidity (passive) or the order initiated the trade and thus took liquidity (aggressive).  This field shall be left blank if not relevant	'PASV' — passive or 'AGRE' — aggressive.
35	Self-Execution Prevention	Indicates if the order has been entered with self-execution prevention criteria, so that it would not execute with an order on the opposite side of the book entered by the same member or participant.	'true' 'false'
36	Trading platform for crypto-asset transaction identification code	For orders executed on trading platform for crypto-assets, alphanumerical code assigned by the trading platform for crypto-assets to the transaction pursuant to [ <i>Delegated Regulation (EU) xx/xxx RTS on order book records</i> ]  The code shall be unique, consistent, and persistent per ISO10383 segment MIC and per trading day.  The components of the transaction identification code shall not disclose the identity of the counterparties to the transaction for which the code is maintained.  For transactions executed by means of transmission within the meaning of Article 1(3) point (a) to an entity providing crypto-asset services outside of the Union, this information shall be recorded where retrievable.	{ALPHANUM-52}
Section J —Indicative auction price and volume			

37	Indicative auction price	The price at which each auction is due to uncross in respect to the crypto-asset for which one or more orders have been placed.	<p>{DECIMAL-18/5} in case the price is expressed as monetary or nominal value.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>DECIMAL-11/10} in case the price is expressed as a percentage or yield</p>
38	Indicative auction volume	The volume (number of units of crypto-asset) that can be executed at the indicative auction price in field 50 if the auction ended at that precise moment of time.	<p>{DECIMAL-18/17} in case the quantity is expressed as number of units</p> <p>{DECIMAL-18/5} in case the quantity is expressed as monetary or nominal value</p>
Section K – Order transmission			



39	Transmitting crypto-asset service provider	In case of transmission of order under Article 11, the LEI code of the transmitting crypto-asset service provider.	{LEI}
40	Transmission of an order indicator	'true' shall be populated by the transmitting firm within the transmitting firm's report where the conditions for transmission specified in Article 11 were not satisfied 'false' – in all other circumstances	'true' 'false'
Section L –Country of residence of the client			
41	Identification of the country of residence	Shall be populated where a client is a resident of a country other than the one of its nationality as described in Article 9.4.	{NATIONAL_ID}  'NOAP'

### SECTION 3

#### Records of transactions

*For the legend, please refer to Section 2, Table 1*

*Table 3*

#### Details of transactions to be kept

Field no	Field	Content to be recorded	Details on transaction data to be provided to the competent authority
1	Transaction status	Indication as to whether the transaction is new or a cancellation.	'NEWT' - New 'CANC' - Cancellation
2	Transaction Record Number	Identification number that is unique to the executing firm for each record	{ALPHANUM-52}
3	Trading platform for crypto-asset transaction identification code	This is a number generated by the trading platform for crypto-asset and disseminated to both the buying and the selling parties in accordance with Article 16 of [RTS under Article 76 of Regulation (EU) 2023/1114]. Where relevant, the transaction hash or other identification alphanumeric string which is automatically generated on the DLT that enables to uniquely identify a specific transaction.	{ALPHANUM-52}
4	Executing entity identification code	Code used to identify the entity executing the transaction.	{LEI}  {ALPHANUM-20}
5	CASP covered by MiCA	Indicates whether the entity identified in Field 4 is a crypto-asset service provider subject to Regulation (EU) 2023/1114.	'true'- yes 'false'- no
6	Buyer identification code	Code used to identify the acquirer of the crypto-asset.  Where the buyer is a legal entity, the LEI code of the acquirer or the alternative identifier referred to in Article 14.3 shall be used.  Where the buyer is a natural person, the identifier specified in Article 9 of this Regulation.  Where the order was transmitted for execution within the meaning of Article 1(3) (a) to a firm performing crypto-asset services outside of the Union, the MIC code of the platform or the LEI or equivalent identifier referred to in Article 14 of the firm shall be used.	{LE'} {ALPHANUM-20} {MIC} {NATIONAL_ID} 'INTC'

		<p>If the crypto-asset service provider executes the transaction on a trading platform located in a third country, the LEI of the buyer, the alternative identifier referred to in Article 14.3 or the National ID shall be recorded.</p> <p>'INTC' shall be used to designate an aggregate client account within the crypto-asset service provider in order to report a transfer into or out of that account with an associated allocation to the individual client(s) out of or into that account respectively.</p>	
7	Country of the branch of the crypto-asset service provider for the buyer	<p>Where the buyer is a client, this field should identify the country of the branch that received the order from the client or made an investment decision for a client in accordance with a discretionary mandate given to it by the client as required by Article 16.</p> <p>Where this activity was not conducted by a branch this should be populated with the country code of the home Member State of the crypto-asset service provider or the country code of the Member State where the crypto-asset service provider has established its registered office.</p>	{COUNTRYCODE_2}
8	Buyer - first name(s)	Full first name(s) of the buyer. In case of more than one first name, all names shall be included in this field separated by a comma.	{ALPHANUM-140}
9	Buyer - surname(s)	Full surname(s) of the buyer. In case of more than one surname, all surnames shall be included in this field separated by a comma.	{ALPHANUM-140}
10	Buyer - date of birth	Date of birth of the buyer.	{DATEFORMAT}
11	Buyer decision maker code	<p>Code used to identify the person who makes the decision to acquire the crypto-asset.</p> <p>Where the decision is made by a crypto-asset service provider, this field shall be populated with the identity of the crypto-asset service provider rather than the individual making the investment decision.</p>	{LEI} {ALPHANUM-20} {NATIONAL_ID}

		<p>Where the decision maker is a legal entity, the LEI code or the alternative identifier referred to in Article 14.3 of the decision maker shall be used.</p> <p>Where the decision maker is not a legal entity, the identifier specified in Article 9 shall be used.</p>	
12	Buy decision maker - First Name(s)	Full first name(s) of the decision maker for the buyer. In case of more than one first name, all names shall be included in this field separated by a comma.	{ALPHANUM-140}
13	Buy decision maker – Surname(s)	Full surname(s) of the decision maker for the buyer. In case of more than one surname, all surnames shall be included in this field separated by a comma.	{ALPHANUM-140}
14	Buy decision maker - Date of birth	Date of birth of the decision maker for the buyer.	{DATEFORMAT}
15	Seller identification code	<p>Code used to identify the disposer of the crypto-asset.</p> <p>Where the seller is a legal entity, the LEI code of the disposer shall be used.</p> <p>Where the seller is not a legal entity, the identifier specified in Article 9 shall be used.</p> <p>Where the order was transmitted for execution within the meaning of Article 1(3) a) to a firm performing crypto-asset services outside of the Union, the MIC code of the platform or the LEI of the firm shall be used.</p> <p>If the crypto-asset service provider executes the transaction on a trading platform located in a third country, the LEI, the alternative identifier referred to in Article 14.3 or the National ID of the seller shall be provided.</p> <p>'INTC' shall be used to designate an aggregate client account within the CASP in order to record a transfer into or out of that account with an associated allocation to the individual client(s) out of or into that account respectively.</p>	{LEI} {ALPHANUM-20} {MIC} {NATIONAL_ID} 'INTC'
16	Country of the branch for the seller	Where the seller is a client, this field should identify the country of the branch that received the order from the client or made an investment decision for a client in	{COUNTRYCODE_2}

		<p>accordance with a discretionary mandate given to it by the client as required by Article 16.</p> <p>Where this activity was not conducted by a branch this should be populated with the country code of the home Member State of the crypto-asset service provider or the country code of the country where the crypto-asset service provider has established its head office or registered office (in the case of third country firms).</p>	
17	Seller - first name(s)	Full first name(s) of the seller. In case of more than one first name, all names shall be included in this field separated by a comma.	{ALPHANUM-140}
18	Seller - surname(s)	Full surname(s) of the seller. In case of more than one surname, all surnames shall be included in this field separated by a comma.	{ALPHANUM-140}
19	Seller - date of birth	Date of birth of the seller	{DATEFORMAT}
20	Seller decision maker code	<p>Code used to identify the person who makes the decision to sell the crypto-asset. Where the decision is made by a crypto-asset service provider, this field shall be populated with the identity of the CASP rather than the individual making the investment decision.</p> <p>Where the decision maker is a legal entity, the LEI code or the alternative identifier referred to in Article 14.3 of the decision maker shall be used.</p> <p>Where the decision maker is a non-legal entity, the identifier specified in Article 9 shall be used.</p>	{LEI} {ALPHANUM-20} {NATIONAL_ID}
21	Sell decision maker - First Name(s)	Full first name(s) of the decision maker for the seller. In case of more than one first name, all names shall be included in this field separated by a comma	{ALPHANUM-140}
22	Sell decision maker – Surname(s)	Full surname(s) of the decision maker for the seller. In case of more than one surname, all surnames shall be included in this field separated by a comma	{ALPHANUM-140}
23	Sell decision maker - Date of birth	Date of birth of the decision maker for the seller	{DATEFORMAT}
24	Transmission of order indicator	<p>‘true’ shall be populated by the transmitting firm within the transmitting firm’s report where the conditions for transmission specified in Article 11 were not satisfied</p> <p>‘false’ – in all other circumstances</p>	<p>‘true’</p> <p>‘false’</p>

25	Transmitting firm identification code for the buyer	Code used to identify the firm transmitting the order This shall be populated by the receiving firm within the receiving firm's report with the identification code provided by the transmitting firm.	{LEI} {ALPHANUM-20}
26	Transmitting firm identification code for the seller	Code used to identify the firm transmitting the order. This shall be populated by the receiving firm within the receiving firm's report with the identification code provided by the transmitting firm	{LEI} {ALPHANUM-20}
27	Trading date time	Date and time when the transaction was executed.  For transactions not executed on a trading venue, the date and time shall be when the parties agree the content of the following fields: quantity, price, currencies in fields 31, 34 and 44, instrument identification code, instrument classification and underlying instrument code, where applicable. For transactions not executed on a trading venue the time recorded shall be at least to the nearest second. Where the transaction results from an order transmitted by the executing firm on behalf of a client to a third party where the conditions for transmission set out in Article 11 were not satisfied, this shall be the date and time of the transaction rather than the time of the order transmission.	{DATE_TIME_FORMAT}
28	Trading capacity	Indicates whether the CASP undertaking the transaction is carrying out matched principal trading, as defined under Article 3(1), point 40 of Regulation (EU) 2023/1114 or exchange of crypto-assets for funds as defined under Article 3(1), point 19 of Regulation (EU) 2023/1114. Where the transaction does not result from the executing firm carrying out matched principal trading or through exchange of crypto-assets for funds, the field shall indicate that the transaction was carried out under any other capacity.	'DEAL' - Exchange of crypto-assets for funds or other crypto-assets 'MTCH' - Matched principal 'AOTC' - Any other capacity
29	Quantity	The number of units of the crypto-assets or the monetary value of the crypto asset. If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.	{DECIMAL-18/17} in case the quantity is expressed as number of units {DECIMAL-18/5} in case the quantity is

		The information reported in this field shall be consistent with the values provided in fields 31 and 32.	expressed as monetary or nominal value
30	Quantity currency	<p>Currency in which the quantity is expressed.</p> <p>Only applicable if quantity is expressed as nominal or monetary value.</p> <p>The quantity shall refer to the crypto-asset units, even when the transaction is denominated in sub-components of that crypto-asset.</p> <p>Where the crypto-asset is traded in electronic money/e-money token, the Digital Token Identifier code or the alternative identifier referred to in Article 15 shall be used.</p>	<p>{CURRENCYCODE_3}</p> <p>{DTI}</p> <p>{ALPHANUM-20}</p>
31	Price	<p>Traded price of the transaction excluding, where applicable, commission, any other fee and accrued interest.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p> <p>Where price is recorded in monetary terms, it shall be provided in the major currency unit.</p> <p>Where price is not applicable, the value shall be 'NOAP' .</p> <p>The information recorded in this field shall be consistent with the values provided in field 30.</p>	<p>{DECIMAL-18/13} in case the price is expressed as monetary value</p> <p>{DECIMAL-11/10} in case the price is expressed as percentage or yield</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP' in case the price is not applicable</p>
32	Price Currency	<p>Currency in which the price is expressed (applicable if the price is expressed as monetary value).</p> <p>Where price of the crypto-asset is expressed in monetary terms and it is expressed in a currency pair, the currency pair in which the price for the crypto-asset related to the order is expressed shall be reported. The first currency code shall be that of the base currency and the second currency code shall be that of the quote currency. The quote currency determines the price of one unit of the base currency. The ISO currency code and the DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI or the alternative</p>	<p>{CURRENCYCODE_3}</p> <p>{DTI}</p> <p>{ALPHANUM-20}</p> <p>{CURRENCYCODE_3} should be used for fiat currencies in a currency pair</p>



		identifier referred to in Article 15 shall be used to represent the fiat currency and the crypto asset respectively in the currency pair.	{DTI_SHORT_NAME} should be used for crypto assets in a currency pair "NOAP"
33	Trading platform for crypto-asset	<p>Identification of the trading platform for crypto-asset where the transaction was executed.</p> <p>Use the ISO 10383 segment MIC for transactions executed on a trading platform for crypto-asset. Where the segment MIC does not exist, use the operating MIC. Use MIC code 'XOFF' for crypto-assets admitted to trading, or traded on a trading platform for crypto-asset or for which a request for admission was made, where the transaction on that crypto-asset is not executed on a trading platform for crypto-asset.</p> <p>Use MIC code 'XXXX' for crypto-assets that are not admitted to trading or traded on a trading platform for crypto-asset or for which no request for admission has been made.-</p>	{MIC}
34	Country of the branch membership	<p>Code used to identify the country of a branch of the crypto-asset service provider whose trading platform for crypto-asset membership was used to execute the transaction.</p> <p>Where a branch's trading platform for crypto-asset membership was not used, this field shall be populated with the country code of the home Member State of the crypto-asset service provider or the country code of the country where the firm has established its head office or registered office (in the case of third country firms).</p> <p>This field shall only be populated for the market side of a transaction executed on a trading platform for crypto-asset.</p>	{COUNTRYCODE_2}
35	Up-front payment	<p>Monetary value of any up-front payment received or paid by the seller.</p> <p>Where the seller receives the up-front payment, the value populated is positive.</p> <p>Where the seller pays the up-front payment, the value populated is negative.</p>	{DECIMAL-18/5}

36	Up-front payment currency	Currency of the up-front payment.	{CURRENCYCODE_3} {DTI} {ALPHANUM-20}
37	Complex trade component id	Identifier, internal to the crypto-asset service provider, to identify all the transaction records related to the same execution of a combination of crypto-assets. The code must be unique at the level of the firm for the group of transaction records related to the execution.	{ALPHANUM-35}
38	Crypto-asset identification code	Code used to identify the crypto-asset This field applies to crypto-assets for which a request for admission to trading has been made, that are admitted to trading or traded on a trading platform for crypto-asset.	{DTI} {ALPHANUM-20}
39	Crypto-asset full name	Full name of the crypto-asset.	{ALPHANUM-350}
40	Crypto-asset classification	Taxonomy used to classify the crypto-asset. or A complete and accurate CFI code shall be provided when available.	ART EMT OT  {CFI_CODE}
41	Investment decision within the crypto-asset service provider	Code used to identify the person or algorithm within the crypto-asset service provider taking the investment decision. The code shall be unique over time for each set of code or trading strategy that constitutes the algorithm and shall be used consistently when referring to the algorithm or version of the algorithm once assigned to it.  For natural persons, the identifier specified in Article 9 shall be used If the investment decision was made by an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity, the field shall be populated as set out in Article 8. Field only applies for investment decision within the firm. Where the transaction is for a transmitted order that has met the conditions for	{NATIONAL_ID} - Natural persons  {ALPHANUM-50} - Algorithms

		transmission set out in Article 11, this field shall be populated by the receiving firm within the receiving firm's record using the information received from the transmitting firm.	
42	Country of the branch responsible for the person making the investment decision	<p>Code used to identify the country of the branch of the crypto-asset service provider for the person taking the investment decision, as set out in Article 16.</p> <p>Where the person taking the investment decision was not supervised by a branch, this field shall be populated with the country code of the home Member State of the crypto-asset service provider or the country code of the Member State where the crypto-asset service provider has established its registered office.</p> <p>Where the transaction is for a transmitted order that has met the conditions for transmission set out in Article 11, this field shall be populated by the receiving firm within the receiving firm's record using the information received from the transmitting firm.</p> <p>This field is not applicable when the investment decision was made by an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity.</p>	{COUNTRYCODE_2}
43	Execution within firm	<p>Code used to identify the person or algorithm automatically determining individual parameters within the crypto-asset service provider for the execution of orders such as whether to initiate the order or its timing, price or quantity.</p> <p>For natural persons, the identifier specified in Article 9 shall be used. If the execution was made by an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity, the field shall be populated as set out in Article 8.</p>	{NATIONAL_ID} - Natural persons {ALPHANUM-50} - Algorithms CLIENT - Client
44	Country of the branch supervising the person determining the conditions for execution	<p>Code used to identify the country of the branch of the crypto-asset service provider for the person determining the execution of the transaction, as set out in Article 16.</p> <p>Where the person responsible was not supervised by a branch, this field shall be populated with the country code of the home Member State of the crypto-asset service provider, or the country code of the country where the crypto-asset service provider has established its registered office.</p>	{COUNTRYCODE_2}

		This field is not applicable when the execution was made by an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its timing, price or quantity.	
45	Short selling indicator	Designation to identify any sale of a crypto-asset which the seller does not own at the time of entering into the agreement to sell including such a sale where at the time of entering into the agreement to sell the seller has borrowed or agreed to borrow the share or debt instrument for delivery at settlement.	'true' 'false'

#### SECTION 4

#### On-chain data

Table 4

#### Details of on-chain data to be kept

Field no	Field	Content to be recorded	Details to be provided to the competent authority
1	Transaction hash	Identifier enabling the unique identification of a specific transaction occurring on the network.	{ALPHANUM-140}
2	Wallet addresses	Code uniquely identifying the wallet, belonging to the buyer/seller, to which the crypto-asset is transferred.	{ALPHANUM-140}
3	Smart Contract Addresses	Code uniquely identifying the smart contract address.	{ALPHANUM-140}

4	Timestamp	Timestamp of the creation of the block.	{DATE_TIME_FORMAT}
5	Quantity/ Current Total Supply	Ratio between the transferred quantity and the current floating amount of the asset.	
6	Token ID	Digital Token Identifier	{DTI}
7	Network fee	Fees which are requested to cover the costs for the creation of a new block.	
8	Fee limit	This is the maximum amount of “network fees” that an on-chain user is willing to pay for the executions of a specific transaction.	
9	Data size	This field is connected to the above. On-chain transaction can contain “attachments” in a specific <i>data</i> field that affect the “network fees” required to process the transaction.	
10	To	The unique identifiers for buyer and seller are usually generated by the DLT protocol on the basis of the buyer/seller wallet addresses.	{ALPHANUM-140}
11	From	The unique identifier for seller usually generated by the DLT protocol on the basis of the seller wallet addresses.	{ALPHANUM-140}
12	Currency	Currency code	{CURRENCYCODE_3} {DTI}
13	Transaction Record Number	Identification number reported in Field 2 of Section 3 that is unique to the executing firm for each record to ensure that a link can be made between the on-chain report and the off-chain one.	{ALPHANUM-140}

## 8.8 Annex VIII: Draft RTS pursuant to Article 76(16)(b) of MiCA

### COMMISSION DELEGATED REGULATION (EU) .../...

of XXX

**supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and format of order book records for crypto-asset service providers operating a trading platform for crypto-assets**

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 Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/193779, and in particular Article 76(16), point (b) thereof,

Whereas:

- (1) Crypto-asset service providers operating platforms for crypto-assets should keep records of relevant data relating to all orders in crypto-assets in an electronic and machine-readable format developed in accordance with the ISO 20022 methodology in order to enable competent authorities to perform effective and efficient collation, comparison and analysis of the relevant order data.
- (2) Since crypto-assets that are not financial instruments are typically neither uniquely identifiable by existing codes which are widely used in financial markets, such as the International Securities Identification Numbers (ISIN), nor describable by using the ISO Classification of Financial Instruments (CFI) code, a new and universal method of identification and classification should be developed. For the purpose of identifying crypto-assets, the European Securities and Markets Authority (ESMA) established by Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>80</sup> considers that the Digital Token Identifier (DTI) is appropriate as it follows the principles of uniqueness, neutrality, reliability, open source, scalability, accessibility on a cost-

---

<sup>79</sup>OJ L 150, 9.6.2023, p. 40.

<sup>80</sup>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).

recovery basis, is offered under an appropriate governance framework and is adopted for use in the Union. For the purpose of classifying crypto-assets, the ISO CFI is being revised to accommodate for the classification of crypto-assets and the revision will not be finalised before the application of this Regulation. Until the revised CFI standard becomes available, an interim taxonomy indicating the type of crypto-assets as prescribed in this Regulation should be used.

- (3) Market abuse behaviours, including market manipulation, may be carried out through various means, including algorithmic trading. Therefore, in order to ensure effective market surveillance, where investment decisions are made by a person other than the client or by a computer algorithm, the person or algorithm should be identified in the order and transaction records using unique, robust and consistent identifiers. Where more than one person makes the investment decision, the person taking the primary responsibility for the decision should be identified in the record.
- (4) In order to ensure unique, consistent and robust identification of natural persons referred to in order records, they should be identified by a concatenation of the country of their nationality followed by identifiers assigned by the country of nationality of those persons. Where those identifiers are not available, natural persons should be identified by identifiers created from a concatenation of their date of birth and name.
- (5) It is necessary that certain personal data are recorded by crypto-asset service providers to identify their clients or other natural persons relevant for orders in crypto-assets, as these data are fundamental to ensure efficient supervision by competent authorities, including in the area of market abuse. In compliance with the principle of data minimisation, such information should be necessary and sufficient to enable the competent authority to carry out a comprehensive assessment of the crypto-asset service provider's compliance with the relevant requirements of Regulation (EU) 2023/1114 and to monitor the trading activity. When processing personal data included in the records, crypto-asset service providers and competent authorities should comply with the relevant provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>81</sup>.
- (6) In order to facilitate market surveillance and to allow comparability of the records, client identification should be reliable, open source, scalable, accessible and, unique across different crypto-asset service providers and in accordance with the internationally established principles of the Financial Stability Board (FSB). In particular, the FSB recommends the use of the unique international Legal Entity Identifier for an unambiguous and consistent identification of all parties to financial transactions. These include members of trading platforms for crypto-assets that are legal entities. In contrast to national/regional codes or names of legal entities, LEI is a widely recognised, financially and operationally accessible international identifier. Only an international

---

<sup>81</sup> 9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).



identifier allows for comparability and aggregation of information at the European level, improving the quality and timeliness of aggregated data and reducing the reporting burden for crypto-asset service providers. Furthermore, without a unique method for the identification and classification of parties and instruments that follow these principles any effort to achieve data-driven market monitoring by competent authorities cannot be achieved. Order records should therefore include the full name and date of birth of clients that are natural persons and should identify clients that are legal entities by their legal entity identifiers (LEIs). In light of the above, where the client does not have a LEI, the records should contain an identifier that ensures similar characteristics.

- (7) Manual or algorithmic abusive behaviours can occur also when determining the trading platform for crypto-asset to access or the crypto-asset service provider to which the orders are to be transmitted or any other conditions related to the execution of the order. Therefore, in order to ensure effective market surveillance, a person or computer algorithm within the crypto-asset service provider that is performing such activities should be identified in the order records. Where both a person and computer algorithm are involved, or more than one person or algorithm is involved, the crypto-asset service provider should determine, on a consistent basis following predetermined criteria, which person or algorithm is primarily responsible for those activities.
- (8) To properly monitor the integrity and stability of the markets in crypto-assets, competent authorities need reliable, consistent and standardised information on the crypto-assets in the order book. Such information should allow them to both identify the individual crypto-asset and classify it according to internationally established principles. In addition, they should be able to retrieve the main characteristics of the crypto-assets, including their technology-specific features. Crypto-asset service providers should therefore use an internationally agreed digital token identifier to identify crypto-assets in the order-book records. As identifier that is internationally agreed and guarantees reliable, consistent, standardised and available information, the Digital Token Identifier (DTI) should be used. Where it is not used, the crypto-asset service provider should record an equivalent unique identifier defined at Union level, meeting certain necessary characteristics including availability. In addition to DTI, the ISO code for the classification of financial instruments (CFI) is currently being revised to accommodate the classification of crypto-assets. Until the time such revision is finalised and the new CFI standard becomes available, an interim classification indicating the type of crypto-assets as prescribed in this Regulation, and consistent with the Commission [*Delegated Regulation (EU) xx/xxx RTS on record keeping of crypto-asset service providers*] should be used.
- (9) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (10) ESMA 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<sup>82</sup>,

HAS ADOPTED THIS REGULATION:

## CHAPTER I

### **Content of records to be kept by crypto-asset services providers operating a trading platform for crypto-assets**

#### *Article 1*

##### **Content, standards and format of relevant order data**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall keep at the disposal of their competent authority the data set out in Articles 3 to 15 of each order in crypto-assets advertised through their systems as specified in Tables 2 and 3 of the Annex insofar as they pertain to the order concerned.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain the data referred to in paragraph 1 in an electronic and machine-readable format in accordance with the ISO 20022 methodology.

#### *Article 2*

##### **Designation to identify natural persons**

1. Crypto-asset service provider operating a trading platform for crypto-assets shall identify natural persons in the order book records by using the designation resulting from the concatenation of the ISO 3166-1 alpha-2 (2 letter country code) of the nationality of the

---

<sup>82</sup> 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).

person, followed by the national client identifier specified in Annex II of Commission Delegated Regulation (EU) 2017/590 based on the nationality of the person.

2. The national client identifier referred to in paragraph 1 shall be assigned in accordance with the priority levels provided in Annex II of Commission Delegated Regulation (EU) 2017/590 using the highest priority identifier that a person has regardless of whether that identifier is already known to the crypto-asset service provider operating a trading platform for crypto-assets.
3. Where a natural person is a national of more than one European Economic Area (EEA) country, the country code of the first nationality when sorted alphabetically by its ISO 3166-1 alpha-2 code and the identifier of that nationality assigned in accordance with paragraph 2 shall be used. Where a natural person has a non-EEA nationality, the highest priority identifier in accordance with the field referring to 'all other countries' provided in Annex II of Commission Delegated Regulation (EU) 2017/590 shall be used. Where a natural person has EEA and non-EEA nationality, the country code of the EEA nationality and the highest priority identifier of that nationality assigned in accordance with paragraph 2 shall be used.
4. Where a natural person is a resident of a country other than the one of its nationality, crypto-asset service providers operating a trading platform for crypto-assets shall also identify natural persons based on the country of residence of the person in the same manner as described in paragraphs 1 to 3.
5. Where the identifier assigned in accordance with paragraph 2 is based on CONCAT, the natural person shall be identified by the crypto-asset service provider operating a trading platform for crypto-assets using the concatenation of the following elements in the following order:
  - (a) the date of birth of the person in the format YYYYMMDD;
  - (b) the five first characters of the first name;
  - (c) the five first characters of the surname.
6. For the purposes of paragraph 4, prefixes to names shall be excluded and first names and surnames shorter than five characters shall be appended by '#' so as to ensure that references to names and surnames in accordance with paragraph 4 contain five characters. All characters shall be in upper case. No apostrophes, accents, hyphens, punctuation marks or spaces shall be used.

### *Article 3*

#### **Identification of the parties involved in the order**

1. For all orders in crypto-assets advertised through their systems, crypto-asset service providers operating a trading platform for crypto-assets shall maintain designations to identify all of the following:
  - (a) the participant to the trading platform for crypto-assets who is eligible for the legal entity identifier code and submits the order to the trading platform for crypto-assets identified in accordance with Article 4;
  - (b) the participant to the trading platform for crypto-assets who is not eligible for the legal entity identifier code and submits the order to the trading platform for crypto-assets, identified as specified in field 2 of Table 2 of the Annex;
  - (c) the client on whose behalf the participant to the trading platform for crypto-assets referred to in points (a) or (b) submits the order to the trading platform for crypto-assets, identified as specified in field 3 of Table 2 of the Annex.
  - (d) the person or the computer algorithm within the participant to the trading platform for crypto-assets referred to in points (a) and (b) that is responsible for the investment decision in relation to the order, identified as specified in field 4 of Table 2 of the Annex.
  - (e) the person or the computer algorithm within the participant to the trading platform for crypto-assets referred to in points (a) and (b) that is responsible for the execution of the order, identified as specified in field 5 of Table 2 of the Annex;
  - (f) the participant to the trading platform for crypto-assets who routes the order on behalf of and in the name of another participant to the trading platform for crypto-assets, identified as a non-executing broker as specified in field 6 of Table 2 of the Annex.
2. For the purposes of point (d) of paragraph 1, where more than one person takes the investment decision, the crypto-asset service provider operating a trading platform for crypto-assets shall keep records of the person taking the primary responsibility for that decision. A crypto-asset service provider operating a trading platform for crypto-assets shall only identify such a person or computer algorithm where that investment decision is made either on behalf of the participant itself, or on behalf of a client in accordance with a discretionary mandate given to it by the client.

3. Where a participant to the trading platform for crypto-assets intends to allocate an order to its client following submission of the order to the trading platform for crypto-assets and has not yet allocated the order to its client at the time of the submission of the order, that client of the participant shall be identified as specified in field 3 of Table 2 of the Annex.
4. Where several orders are submitted to the trading platform for crypto-assets together as an aggregated order, the information referred to in field 3 of Table 2 of the Annex shall be recorded in respect of each client.

#### *Article 4*

##### **Identification of participants that are legal entities**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall identify participants that are legal entities by using the legal entity identifier provided by that participant as specified in field 1 of Table 2 of the Annex.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall record the legal entity identifier of any participants eligible for the legal entity identifier.
3. The crypto-asset service provider operating a trading platform for crypto-assets shall ensure that the length and construction of the legal entity identifier code are compliant with the ISO 17442 standard and that the code is included in the Global LEI database maintained by the Central Operating Unit appointed by the Regulatory Oversight Committee and pertains to the entity concerned.
4. Where the participant does not have a legal entity identifier compliant with the ISO 17442 standard, the crypto asset service provider shall obtain the ISO 17442 for the participant or use an identifier as defined at Union level which meets all of the following characteristics:
  - (a) is unique;
  - (b) is neutral;
  - (c) is reliable;
  - (d) is open source;
  - (e) is scalable;
  - (f) is accessible;
  - (g) is available at a reasonable cost, and

(h) is subject to an appropriate governance framework.

#### *Article 5*

### **Trading capacity of participants of the trading platform for crypto-assets**

1. The trading capacity in which the participant of the trading platform for crypto-assets submits an order shall be described as specified in field 7 of Table 2 of the Annex.

#### *Article 6*

### **Date and time recording**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of the date and time of the occurrence of each event listed in field 21 of Table 2 of the Annex as specified in field 9 of Table 2 of the Annex.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of the date and time for each data element listed in fields 48, 49 and 50 of Table 2 of the Annex, as specified in field 9 of Table 2 of the Annex.

#### *Article 7*

### **Validity period and order restrictions**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall keep a record of the validity periods and order restrictions that are listed in fields 10 and 11 of Table 2 of the Annex.
2. Records of the dates and times in respect of validity periods shall be maintained for each validity period as specified in field 12 of Table 2 of the Annex.

#### *Article 8*

### **Priority and sequence numbers**

1. Crypto-asset service providers operating a trading platform for crypto-assets which operate trading systems on a price visibility-time priority shall maintain a record of the priority time stamp for all orders as specified in field 13 of Table 2 of the Annex. The priority time stamp shall be maintained with the same level of accuracy specified in field 9 of Table 2 of the Annex.
2. Crypto-asset service providers operating a trading platform for crypto-assets which operate trading systems on a size-time priority basis shall maintain a record of the

quantities which determine the priority of orders as specified in field 14 of Table 2 of the Annex and the priority time stamp referred to in paragraph 1.

3. Crypto-asset service providers operating a trading platform for crypto-assets which use a combination of price-visibility-time priority and size-time priority and display orders on their order book in time priority shall comply with paragraph 1.
4. Crypto-asset service providers operating a trading platform for crypto-assets which use a combination of price-visibility-time priority and size-time priority and display orders on their order book in size-time priority shall comply with paragraph 2.
5. Crypto-asset service providers operating a trading platform for crypto-assets shall assign and maintain a sequence number for each event as specified in field 15 of Table 2 of the Annex.

#### *Article 9*

#### **Identification codes for orders in crypto-assets**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain an individual identification code for each order as specified in field 20 of Table 2 of the Annex. The identification code shall be unique per order book, per trading day and per crypto-asset. It shall apply from the receipt of the order by the operator of the trading platform for crypto-assets until the removal of the order from the order book. The identification code shall also apply to rejected orders irrespective of the ground for their rejection.
2. The operator of the trading platform for crypto-assets shall maintain the relevant details of strategy orders with implied functionality (SOIF) that are disseminated to the public as specified in the Annex. Field 32 of Table 2 of the Annex shall include a statement that the order is an implicit order.
3. Upon execution of a SOIF, its details shall be maintained by the operator of the trading platform for crypto-assets as specified in the Annex.
4. Upon execution of a SOIF, a strategy linked order identification code shall be indicated using the same identification code for all orders connected to the particular strategy. The strategy linked order identification code shall be as specified in field 45 of Table 2 of the Annex.
5. Orders submitted to a trading platform for crypto-assets allowing for a routing strategy shall be identified by that trading platform for crypto-assets as 'routed' as specified in field 32 of Table 2 of the Annex when they are routed to another trading platform for crypto-assets. Orders submitted to a trading platform for crypto-assets allowing for a routing strategy shall

retain the same identification code for their lifetime, regardless of whether any remaining quantity is re-posted on the order book of entry.

*Article 10*

**Events affecting the orders in crypto-assets**

Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of the details referred to in field 21 of Table 2 of the Annex in relation to the new orders.

*Article 11*

**Type of order in crypto-assets**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of the order type for each order received using their own classification as specified in field 22 of Table 2 of the Annex.
2. Crypto-asset service providers operating a trading platform for crypto-assets shall classify each order received either as a limit order or as a stop order as specified in field 23 of Table 2 of the Annex.

*Article 12*

**Prices relating to orders**

Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of all price-related details referred to in Section I of Table 2 of the Annex insofar as they pertain to the orders.

*Article 13*

**Order instructions**

Crypto-asset service providers operating a trading platform for crypto-assets shall maintain records of all order instructions received for each order as specified in Section J of Table 2 of the Annex.

*Article 14*

**Trading platform for crypto-assets transaction identification code**



1. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain an individual transaction identification code for each transaction resulting from the full or partial execution of an order as specified in field 47 of Table 2 of the Annex or field 1 of Table 3.

*Article 15*

**Trading phases and indicative auction price and volume**

1. Crypto-asset service providers operating a trading platform for crypto-assets shall maintain a record of the order details as specified in Section K of Table 2 of the Annex.
2. Where competent authorities request details referred to in Section K, the details referred to in fields 9 and 15 to 18 of Table 2 of the Annex shall also be considered as details pertaining to the order concerned by that request.

*Article 16*

**Entry into force and application**

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,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

*ANNEX*

*Table 1*

**Legend for Table 2**

Symbol	Data type	Definition
{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{CFI_CODE}	6 characters	ISO 10962 CFI code.
{COUNTRYCODE_2}	2 alphanumerical characters	2 letter country code, as defined by ISO 3166-1 alpha-2 country code
{CURRENCYCODE_3}	3 alphanumerical characters	3 letter currency code, as defined by ISO 4217 currency codes

{DATE_TIME_FORM AT}	ISO 8601 date and time format	<p>Date and time in the following format:          YYYY-MM-DDThh:mm:ss.dddZ.</p> <ul style="list-style-type: none"> <li>– ‘YYYY’ is the year;</li> <li>– ‘MM’ is the month;</li> <li>– ‘DD’ is the day;</li> <li>– ‘T’ – means that the letter ‘T’ shall be used</li> <li>– ‘hh’ is the hour;</li> <li>– ‘mm’ is the minute;</li> <li>– ‘ss.ddd’ is the second and its fraction of a second;</li> <li>– Z is UTC time.</li> </ul> <p>Dates and times shall be reported in UTC.</p>
{DATEFORMAT}	ISO 8601 date format	Dates shall be formatted in the following format: YYYY-MM-DD.
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	<p>Numerical field for both positive and negative values.</p> <ul style="list-style-type: none"> <li>– decimal separator is ‘.’ (full stop);</li> <li>– negative numbers are prefixed with ‘-’ (minus); Values are rounded and not truncated.</li> </ul>
{DTI}	9 alphanumeric characters	ISO 24165 DTI code assigned to fungible digital assets which uses distributed ledger technology for its issuance, storage, exchange, record of ownership or transaction validation and is not a currency (ISO 4217) as described in ISO 24165 - DTI.

{DTI_SHORT_NAME }	n alphanumeric characters	DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI
{INTEGER-n}	Integer number of up to n digits in total	Numerical field for both positive and negative integer values.
{ISIN}	12 alphanumeric characters	ISIN code, as defined in ISO 6166
{LEI}	20 alphanumeric characters	Legal entity identifier as defined in ISO 17442

{MIC}	4 alphanumerical characters	Market identifier as defined in ISO 10383
{NATIONAL_ID}	35 alphanumerical characters	The identifier is derived in accordance with Article 3 and Annex II of Commission Delegated Regulation (EU) 2017/590.

*Table 2*

<b>Field Number</b>	<b>Field Name</b>	<b>Field description</b>	<b><i>Details of the order book</i></b>
<b>Section A — Identification of the relevant parties</b>			
1	Identification of the entity which submitted the order.	The identity of the participant of the trading platform operated by the crypto-asset service provider or equivalent as specified in Article 4. This field only applies to entities eligible for a legal entity identifier (LEI).	{LEI} {ALPHANUM-20}
2	Identification of the participants which submitted the order.	The identity of the participant of the trading platform operated by the crypto-asset service provider. This field applies to participants that are not eligible for an LEI.	{NATIONAL_ID}

3	Client identification code	<p>Code used to identify the client of the participant to the trading platform for crypto-assets.</p> <p>Where the client is a legal entity, the LEI code or the alternative identifier referred to in Article 4.4 {ALPHANUM-20} of the client shall be used.</p> <p>Where the client is not a legal entity, the {NATIONAL_ID} shall be used.</p> <p>In case of pending allocations, the flag PNAL as specified in Article 3 of this Regulation shall be used.</p> <p>This field shall be populated with 'NOAP' only where the participant of the trading platform for crypto-assets crypto-asset service provider has a direct interest to buy or sell.</p>	{LEI} {ALPHANUM-20} {NATIONAL_ID} 'PNAL' 'NOAP'
4	Investment decision within the CASP	<p>Code used to identify the person or the algorithm within the crypto-asset service provider who is responsible for the investment decision.</p> <p>Where a natural person within the crypto-asset service provider is responsible for the investment decision the person who is responsible or has primary responsibility for the investment decision shall be identified with the {NATIONAL_ID}</p> <p>Where an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its the timing, price or quantity was responsible for the investment decision, the field shall be populated with a code assigned according to Article 3.</p> <p>This field shall be left blank when the investment decision was not made by a person or algorithm within the crypto-asset service provider.</p>	{NATIONAL_ID} — Natural persons {ALPHANUM-50} — Algorithms
5	Execution within firm	<p>Code used to identify the person or algorithm within the crypto-asset service provider who is responsible for the execution of the transaction resulting from the order. This field is not applicable when the executing entity is a natural person.</p> <p>Where a natural person is responsible for the execution of the transaction, the person shall be identified by {NATIONAL_ID}</p>	{NATIONAL_ID} — Natural persons {ALPHANUM-50} — Algorithms

		<p>Where an algorithm automatically determining individual parameters of orders such as whether to initiate the order or its the timing, price or quantity is responsible for the execution of the transaction, this field shall be populated with a code assigned by the crypto-asset service provider, in accordance with Article 3.</p> <p>Where more than one person or a combination of persons and algorithms are involved in the execution of the transaction, the crypto-asset service provider shall determine the trader or algorithm primarily responsible and populate this field with the identity of that trader or algorithm</p>	
6	Non-executing broker	<p>The code used to identify a participant of the trading platform for crypto-assets who routed an order on behalf of and in the name of another participant of the trading platform for crypto-assets.</p> <p>This field shall be 'NOAP' when not relevant.</p>	<p>LEI {ALPHANUM-20} 'NOAP'</p>
Section B — Trading capacity and liquidity provision			
7	Trading capacity	<p>Indicates whether the crypto-asset service provider undertaking the transaction is carrying out matched principal trading, as defined under Article 3(1), point 40 of Regulation (EU) 2023/1114 or exchanging crypto-assets for funds as defined under Article 3(1), point 19 of Regulation (EU) 2023/1114.</p> <p>Where the order submission does not result from the crypto-asset service provider carrying out matched principal trading or exchanging crypto-assets for funds, the field shall indicate that the transaction was carried out under any other capacity.</p>	<p>'DEAL' — Exchanging crypto-assets for funds 'MTCH' — Matched principal 'AOTC' — Any other capacity</p>
Section C — Date and time			
9	Date and Time	The date and time for each event listed in Sections G and K of this Table.	{DATE_TIME_FORMAT}
Section D — Validity period and order restrictions			

10	Validity period	<p>Good-For-Day: the order expires at the end of the trading day on which it was entered in the order book</p> <p>Good-Till-Cancelled: the order will remain active in the order book and be executable until it is actually cancelled.</p> <p>Good-Till-Time: the order expires at the latest at a pre-determined time within the current trading session.</p> <p>Good-Till-Date: the order expires at the end of a specified date.</p> <p>Good-Till-Specified Date and Time: the order expires at a specified date and time.</p> <p>Good After Time: the order is only active after a pre-determined time within the current trading session.</p> <p>Good After Date: the order is only active from the beginning of a pre-determined date.</p> <p>Good After Specified Date and Time: the order is only active from a pre-determined time on a pre-determined date.</p> <p>Immediate-Or-Cancel: an order which is executed upon its entering into the order book (for the quantity that can be executed) and which does not remain in the order book for the remaining quantity (if any) that has not been executed.</p> <p>Fill-Or-Kill: an order which is executed upon its entering into the order book provided that it can be fully filled: in the event the order can only be partially executed, then it is automatically rejected and cannot therefore be executed.</p> <p>Other: any additional indications that are unique for specific business models, trading platforms or systems.</p>	<p>'DAVY' — Good-For-Day</p> <p>'GTCV' — Good-Till-Cancelled</p> <p>'GTTV' — Good-Till-Time</p> <p>'GTDV' — Good-Till-Date</p> <p>'GTSV' — Good-Till-Specified Date and Time</p> <p>'GATV' — Good After Time</p> <p>'GADV' — Good After Date</p> <p>'GASV' — Good After Specified Date and Time</p> <p>'IOCV' — Immediate-Or-Cancel</p> <p>'FOKV' — Fill-Or-Kill</p> <p>or</p> <p>{ALPHANUM-4} characters not already in use for the trading platform for crypto-</p>
----	-----------------	---	---



			assets' own classification.
11	Order restriction	<p>Good For Closing Price Crossing Session: where an order qualifies for the closing price crossing session.</p> <p>Valid For Auction: the order is only active and can only be executed at auction phases (which can be pre-defined by the crypto-asset service provider client who submitted the order, e.g. opening and/closing auctions and/or intraday auction).</p> <p>Valid For Continuous Trading only: the order is only active during continuous trading.</p> <p>Other: any additional indications that are unique for specific business models, trading platforms or systems.</p>	<p>'SESR' — Good For Closing Price Crossing Session</p> <p>'VFAR' — Valid For Auction</p> <p>'VFCR' — Valid For Continuous Trading only</p> <p>{ALPHANUM-4} characters not already in use for the trading platform for crypto-assets' own classification.</p> <p>This field shall be populated with multiple flags separated by a comma where more than one flag is applicable</p>

12	Validity period and time	<p>This field refers to the time stamp reflecting the time on which the order becomes active or it is ultimately removed from the order book:</p> <p>Good for day: the date of entry with the timestamp immediately prior to midnight</p> <p>Good till time: the date of entry and the time to that specified in the order</p> <p>Good till date: will be the specified date of expiry with the timestamp immediately prior to midnight</p> <p>Good till specified date and time: the specified date and time of expiry</p> <p>Good after time: the date of entry and the specified time at which the order becomes active</p> <p>Good after date: the specified date with the timestamp immediately after midnight</p> <p>Good after specified date and time: the specified date and time at which the order becomes active</p> <p>Good till Cancel: the ultimate date and time the order is automatically removed by market operations</p> <p>Other: timestamp for any additional validity type.</p>	{DATE_TIME_FORMAT}
Section E — Priority and sequence number			
13	Priority time stamp	This field shall be updated every time the priority of an order changes	{DATE_TIME_FORMAT}
14	Priority size	<p>For trading platforms for crypto-assets which use size-time priority, this field shall be populated with a positive number corresponding to the quantity.</p> <p>This field shall be updated every time the priority of the order changes.</p>	Up to 20 numeric positive digits.
15	Sequence number	Each event listed in section G shall be identified using positive integers in ascending order.	{INTEGER-50}

		The sequence number shall be unique to each type of event; consistent across all events, timestamped by the operator of the trading platform for crypto-assets; be persistent for the date that the event occurs.	
Section F — Identification of the order			
16	Segment MIC code	<p>Identification of the trading platform for crypto-asset where the order was submitted.</p> <p>If the trading platform for crypto-asset uses segment MICs then the segment MIC shall be used.</p> <p>If the trading platform for crypto-asset does not use segment MICs then the operating MIC shall be used</p>	{MIC}
17	Order book code	The alphanumerical code established by the trading platform for crypto-assets for each order book. An order book shall be understood as an organised list of buy and sell orders for a specific crypto-asset.	{ALPHANUM-20}
18	Crypto-asset identification code	<p>Unique and unambiguous identifier of the crypto-asset in accordance with Article 15 of [Delegated Regulation (EU) xx/xxx RTS on record keeping]</p>	{DTI} {ALPHANUM-20}
19	Date of receipt	Date of receipt of the original order	{DATEFORMAT}
20	Order identification code	An alphanumerical code assigned by the operator of the trading platform for crypto-assets to the individual order.	{ALPHANUM-50}
Section G — Events affecting the order			
21	New order, order modification, order	New order: submission of a new order to the crypto-asset service provider operating the trading platform for crypto-assets.	'NEWO' — New order 'TRIG' — Triggered

	<p>cancellation, order rejections, partial or full execution</p>	<p>Triggered: an order which becomes executable or, as the case may be, non-executable upon the realisation of a pre-determined condition.</p> <p>Replaced by the participant of the trading platform for crypto-assets: where a participant or client of the trading platform for crypto-assets decides upon its own initiative to change any characteristic of the order it has previously entered into the order book.</p> <p>Replaced by market operations (automatic): where any characteristic of an order is changed by the trading platform for crypto-assets operator's ICT systems. This includes where a peg order's or a trailing stop order's current characteristics are changed to reflect how the order is located within the order book.</p> <p>Replaced by market operations (human intervention): where any characteristic of an order is changed by a trading platform for crypto-assets operator's staff. This includes the situation where a participant of the trading platform for crypto-assets requests to urgently cancel the orders linked to ICT incidents.</p> <p>Change of status at the initiative of the participant of the trading platform for crypto-assets. This includes activation and deactivation.</p> <p>Change of status due to market operations.</p> <p>Cancelled at the initiative of the participant of the trading platform for crypto-assets; where a participant or client decides upon its own initiative to cancel the order it has previously entered.</p> <p>Cancelled by market operations.</p> <p>Rejected order: an order received but rejected by the operator of the trading platform for crypto-assets.</p> <p>Expired order: where the order is removed from the order book upon the end of its validity period.</p>	<p>'REME' — Replaced by the member or participant of the trading platform for crypto-assets</p> <p>'REMA' — Replaced by market operations (automatic)</p> <p>'REMH' — Replaced by market operations (human intervention)</p> <p>'CHME' — Change of status at the initiative of the participant of the trading platform for crypto-assets</p> <p>'CHMO' — Change of status due to market operations</p> <p>'CAME' — Cancelled at the initiative of the participant of the trading platform for crypto-assets</p> <p>'CAMO' -Cancelled by market operations</p>
--	--	---	---

		<p>Partially filled: where the order is not fully executed so that there remains a quantity to be executed-</p> <p>Filled: where there is no more quantity to be executed.</p>	<p>‘REMO’ — Rejected order</p> <p>‘EXPI’ — Expired order</p> <p>‘PARF’ — Partially filled</p> <p>‘FILL’ — Filled</p> <p>{ALPHANUM-4} characters not already in use for the trading platform for crypto-assets’ own classification.</p>
Section H — Type of order			
22	Order type	Identifies the type of order submitted to the trading platform for crypto-assets as per the trading platform for crypto-assets’ specifications.	{ALPHANUM-50}
23	Order type classification	<p>Classification of the order according to two generic order types. LIMIT order: in the cases where the order is tradable and</p> <p>STOP order: in the cases where the order becomes tradable only upon the realisation of a pre-determined price event.</p>	The letters ‘LMTO’ for limit or the letters ‘STOP’ for stop.
Section I — Prices			
24	Limit price	The maximum price at which a buy order can trade or the minimum price at which a sell order can trade.	{DECIMAL-18/13} in case the price is

		<p>The spread price for a strategy order. It can be negative or positive.</p> <p>This field shall be 'NOAP' when not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>expressed as monetary value.</p> <p>{DECIMAL-11/10} in case the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
25	Additional limit Price	<p>Any other limit price which may apply to the order. This field shall be 'NOAP' if not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10} where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>

26	Stop price	<p>The price that must be reached for the order to become active.</p> <p>For stop orders triggered by events independent of the price of the crypto-asset, this field shall be populated with a stop price equal to zero.</p> <p>This field shall be 'NOAP' if not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10} where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
27	Pegged limit price	<p>The maximum price at which a pegged order to buy can trade or the minimum price at which a pegged order to sell can trade.</p> <p>This field shall be 'NOAP' if not relevant.</p> <p>Where price is reported in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p> <p>If the price is expressed in sub-components of that crypto-asset, it shall be nonetheless recorded in decimal notation of the price expressed in units of that crypto-asset.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10} where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>

28	Transaction price	<p>Traded price of the transaction excluding, where applicable, commission, other fees and accrued interest.</p> <p>Where price is not applicable the field shall be populated with the value 'NOAP'.</p> <p>Where price is recorded in monetary terms, it shall be provided in the major currency unit.</p> <p>If the crypto-asset is traded based on a currency pair the price shall express the quantity of the quote currency for one unit of the base currency.</p>	<p>{DECIMAL-18/13} where the price is expressed as a monetary value.</p> <p>{DECIMAL-11/10} where the price is expressed as a percentage or yield.</p> <p>{DECIMAL-18/17} in case the price is expressed as basis points</p> <p>'NOAP'</p>
29	Price currency	<p>Currency in which the trading price for the crypto-asset related to the order is expressed (applicable where the price is expressed as monetary value).</p> <p>Where the crypto-asset is traded in electronic money/e-money token, the Digital Token Identifier code shall be used.</p> <p>Where price of the crypto-asset is expressed in monetary terms and it is expressed in a currency pair, the currency pair in which the price for the crypto-asset related to the order is expressed shall be reported. The first currency code shall be that of the base currency and the second currency code shall be that of the quote currency. The quote currency determines the price of one unit of the base currency. The ISO currency code and the DTI short name as registered according to the ISO 24165-2 data elements for registration of the DTI or the alternative equivalent identifier referred to in Article 15 of [<i>Delegated Regulation xx/xxx RTS on record keeping</i>] shall be used to represent the fiat currency and the crypto asset respectively in the currency pair.</p>	<p>{CURRENCYCODE_3}</p> <p>{DTI}</p> <p>{ALPHANUM-20}</p> <p>{CURRENCYCODE_3} should be used for fiat currencies in a currency pair</p> <p>{DTI_SHORT_NAME} should be used for crypto assets in a currency pair</p> <p>'NOAP'</p>



30	Price notation	Indicates whether the price is expressed in monetary value, in percentage, in yield, in basis points or in crypto-assets.	'MONE' — Monetary value 'PERC' — Percentage 'YIEL' — Yield 'BAPO' — Basis points
Section J — Order instructions,			
31	Buy-sell indicator	To record if the order is to buy or sell.	'BUYI' — buy 'SELL' — sell
32	Order status	<p>To identify orders that are active/inactive/suspended, firm/indicative (assigned to quotes only)/implicit/rerouted.</p> <p>Active — non-quote orders that are tradable.</p> <p>Inactive — non-quote orders that are not tradable.</p> <p>Firm/Indicative — Assigned to quotes only. Indicative quotes mean that they are visible but cannot be executed. This includes warrants in some trading platform for crypto-assets. Firm quotes can be executed.</p> <p>Implicit — Used for strategy orders that are derived from implied in or implied out functionality.</p> <p>Routed — Used for orders that are routed by the trading platform for crypto-assets to other venues.</p>	'ACTI'- active or 'INAC'- inactive or 'FIRM'- firm quotes or 'INDI'- indicative quotes or 'IMPL'- implied strategy orders

			or 'ROUT'- routed orders. If multiple statuses are applicable, this field shall be populated with multiple flags separated by comma
33	Quantity notation	Indicates whether the quantity reported is expressed in number of units, as a nominal value or as a monetary value, or crypto-asset units.	'UNIT' — Number of units 'NOML' — Nominal value 'MONE' — Monetary value '{CRYP}' — Value in crypto-assets
34	Quantity currency	Currency in which the quantity is expressed. The currency shall refer to the crypto-asset units, even when the transaction is denominated in sub-components of that crypto-asset.  Field only needs to be populated where the quantity is expressed as a nominal monetary value or crypto-asset units.	{CURRENCYCODE_3} {DTI} {ALPHANUM-20}
35	Initial quantity	The number of units of the crypto-asset in the order. In case the order pertains a fraction of a crypto-asset, indicate the quantity in decimal notation of the unit.  The nominal or monetary value of the crypto-asset.	{DECIMAL-18/17} in case the quantity is

			expressed as number of units {DECIMAL-18/5} in case the quantity is expressed as monetary or nominal value
36	Remaining quantity	<p>The total quantity that remains in the order book after a partial execution or in the case of any other event affecting the order.</p> <p>On a partial fill order event, this shall be the total remaining volume after that partial execution. On an order entry this shall equal the initial quantity.</p>	<p>{DECIMAL-18/17} in case the quantity is expressed as a number of units</p> <p>{DECIMAL-18/5} where the quantity is expressed as monetary or nominal value</p>
37	Displayed quantity	The quantity that is visible (as opposed to hidden) in the order.	<p>{DECIMAL-18/17} in case the quantity is expressed as a number of units</p> <p>{DECIMAL-18/5} where the quantity is</p>

			expressed as monetary or nominal value
38	Traded quantity	Where there is a partial or full execution, this field shall be populated with the executed quantity.	{DECIMAL-18/17} in case the quantity is expressed as a number of units {DECIMAL-18/5} where the quantity is expressed as monetary or nominal value
39	Minimum Acceptable Quantity (MAQ)	The minimum acceptable quantity for an order to be filled which can consist of multiple partial executions and is normally only for non-persistent order types. This field shall be 'NOAP' if not relevant.	{DECIMAL-18/17} in case the quantity is expressed as a number of units {DECIMAL-18/5} where the quantity is expressed as monetary or nominal value 'NOAP'

40	Minimum executable size (MES)	The minimum execution size of any individual potential execution. This field shall be left blank if not relevant.	{DECIMAL-18/17} in case the quantity is expressed as a number of units {DECIMAL-18/5} where the quantity is expressed as monetary or nominal value
41	MES first execution only	Specifies whether the MES is relevant only for the first execution. This field can be left blank where field 40 is left blank.	'true' 'false'
42	Passive only indicator	Indicates if the order is submitted to the trading platform for crypto-asset with a characteristic/flag, such that the order shall not immediately execute against any contra visible orders.	'true' 'false'
43	Passive or aggressive indicator	On partial fill and fill order events, indicates whether the order was already resting on the order book and providing liquidity (passive) or the order initiated the trade and thus took liquidity (aggressive). This field shall be left blank if not applicable.	'PASV' — passive or 'AGRE' — aggressive.
44	Self-Execution Prevention	Indicates if the order has been entered with self-execution prevention criteria, so that it would not execute with an order on the opposite side of the book entered by the same participant.	'true' 'false'

45	Strategy Linked Order identification	The alphanumerical code used to link all connected orders that are part of a strategy pursuant to Article 9(2).	{ALPHANUM-50}
46	Routing Strategy	The applicable routing strategy as per the trading platform for crypto-assets' specification. This field shall be left blank if not applicable.	{ALPHANUM-50}
47	Trading platform for crypto-assets transaction identification code	Alphanumerical code assigned by the trading platform for crypto-asset to the transaction pursuant to Article 14.  The code shall be unique, consistent, and persistent per ISO10383 segment MIC and per trading day. The components of the transaction identification code shall not disclose the identity of the counterparties to the transaction for which the code is maintained. For orders transmitted to trading platforms for crypto-assets as referred to in Articles 12 and 13 of RTS pursuant to Article 68(10)(b) to an entity providing crypto-asset services outside of the Union, this information shall be recorded whenever those are retrievable.	{ALPHANUM-52}
Section K — Trading phases, indicative auction price and volume			
48	Trading phases	The name of each of the different trading phases during which an order is present in the order book including trading halts, circuit breakers and suspensions.	{ALPHANUM-50}
49	Indicative auction price	The price at which each auction is due to uncross in respect to the crypto-asset for which one or more orders have been placed.	{DECIMAL-18/5} in case the price is expressed as monetary or nominal value.  Where price reported in monetary terms, it shall

			be provided in the major currency unit. {DECIMAL-11/10} in case the price is expressed as a percentage or yield
50	Indicative auction volume	The volume (number of units of the crypto-asset) that can be executed at the indicative auction price in field 50 if the auction ended at that precise moment of time.	{DECIMAL-18/17} in case the quantity is expressed as number of units {DECIMAL-18/5} in case the quantity is expressed as monetary or nominal value
<b>Section L – Country of residence of natural persons</b>			
51	Identification of the country of residence	Shall be populated where a natural person is a resident of a country other than the one of its nationality as described in Article 2.4.	{NATIONAL_ID} 'NOAP'

*Table 3*  
**On-chain data**

Field no	FIELD	CONTENT TO BE RECORDED	Details to be provided to the competent authority
1	Transaction hash	Identifier enabling the unique identification of a specific transaction occurring on the network.	{ALPHANUM-140}
2	Wallet addresses	Code uniquely identifying the wallet, belonging to the buyer/seller, to which the crypto-asset is transferred.	{ALPHANUM-140}
3	Smart Contract Addresses	Code uniquely identifying the smart contract address.	{ALPHANUM-140}
4	Timestamp	Timestamp of the creation of the block.	{DATE_TIME_FORMAT}
5	Quantity/ Current Total Supply	Ratio between the transferred quantity and the current floating amount of the asset.	
6	Token ID	Digital Token Identifier or the alternative equivalent identifier referred to in Article 15 of [ <i>Delegated Regulation (EU) xx/xxx RTS on record keeping</i> ]	{DTI} {ALPHANUM-20}
7	Network fee	Fees which are requested to cover the costs for the creation of a new block.	
8	Fee limit	This is the maximum amount of “network fees” that an on-chain user is willing to pay for the executions of a specific transaction.	
9	<i>DataSize</i>	This field is connected to the above. An on-chain transaction can contain “attachments” in a specific <i>data</i> field that affect the “network fees” required to process the transaction.	
10	<i>“To”</i>	The unique identifier for buyer usually generated by the DLT protocol on the basis of the buyer wallet addresses.	{ALPHANUM-140}
11	<i>“from”</i>	The unique identifier for seller usually generated by the DLT protocol on the basis of the seller wallet addresses.	{ALPHANUM-140}
12	Currency	Currency code	{CURRENCYCODE_3} {DTI} {ALPHANUM-20}



<b>13</b>	Transaction Record Number	Identification number reported in Field 2 of Section 3 that is unique to the executing firm for each record to ensure that a link can be made between the on-chain report and the off-chain one.	{ALPHANUM-140}
-----------	---------------------------	--	----------------

## 8.9 Annex IX: Draft ITS pursuant to Articles 6, 19 & 51 of MiCA

### COMMISSION IMPLEMENTING REGULATION (EU) 2024/XXX

of XXXX

**laying down implementing technical standards for the application of Regulation (EU) No 2023/1114 of the European Parliament and of the Council with regard to forms, formats and templates for the crypto-asset white papers**

**(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<sup>83</sup>, and in particular Articles 6(11) third subparagraph, 19(10) third subparagraph and 51(10) third subparagraph thereof,

Whereas:

- (1) Regulation (EU) 2023/1114 requires that, when drawing up a crypto asset white paper, issuers of crypto-assets, offerors, persons seeking admission to trading and operators of a trading platform admitting to trading a crypto-asset ensure that such a crypto-asset white paper contains information which is relevant to enable investors to make an informed investment decision and to make such white papers available in a machine-readable format.
- (2) The adoption of standardised templates for reporting such information ensures a high level of transparency and comparability of white papers, thus ensuring that investors in crypto-assets are appropriately informed about the characteristics and risks of the crypto-assets they invest in, of the issuer and of the offer or admission to trading.
- (3) In order to remove duplicative requirements and reduce the compliance burden, the data fields related to information about the persons drawing up a crypto-asset white paper which are retrievable from the Global Legal Entity Identifier Foundation (GLEIF) database should not be applicable if a valid Legal Entity Identifier Code is provided in

---

<sup>83</sup> OJ L 150, 9.6.2023, p. 40.

the white paper. These fields pertain to the following information: legal form, registered address and head office (where different) and identity of the parent company.

- (4) In order to ensure a unique and consistent identification of the Crypto-Asset Service Provider (CASP), a CASP identifier is necessary in addition to the CASP name. To obtain authorisation as a CASP, a valid Legal Entity Identifier (LEI) is required as per Article 62 paragraph 2, point (a) of Regulation (EU) 2023/1114. Therefore, it is expected that the LEI will always be available for the identification of CASPs.
- (5) In order to remove duplicative requirements and reduce the compliance burden, the data fields related to information to be included in a crypto-asset white paper, which are retrievable from the Digital Token Identifier Foundation Registry (DTIF) database should not be applicable if a valid Digital Token Identifier is provided in the white paper. These fields pertain to the following information: crypto-assets name, abbreviation, commercial name or trading name, and digital ledger technology.
- (6) In order to provide information on the expenses related to the public offering of asset-referenced tokens or of crypto-asset other than asset-referenced tokens and e-money tokens should consider all the fees paid to guarantors, underwriters and similar.
- (7) In order to further facilitate their analysis and comparability, the white papers should be marked up using eXtensible Business Reporting Language (XBRL). XBRL is a machine-readable format which allows for the automated consumption of large amount of information. It is well established and in use in a number of jurisdictions.
- (8) In order to ensure the protection of retail investors, it is important that white papers are human readable and easily accessible without specialised software. The use of Inline XBRL technology for embedding XBRL markups in XHTML documents enables such documents to be at the same time machine-readable and human readable.
- (9) The use of XBRL requires the development of a taxonomy. The elements of the taxonomy to be used for the white papers should be exclusively the fields included in the standardised templates.
- (10) The taxonomy for the use of XBRL is accessed in the form of XBRL files ('XBRL taxonomy files'), which provide a structured representation of the fields to be reported. The fields and their appropriate data type should be made available in a simple human-readable form in this Regulation. It is important that persons drawing up a white paper use XBRL taxonomy files that are compliant with all relevant technical and legal requirements. To facilitate compliance and to enhance transparency, the European Securities and Markets Authority ('ESMA') may publish the XBRL taxonomy files on its website in a machine-readable and freely downloadable format.
- (11) It is necessary to enable persons drawing up the whitepapers to adapt to the requirements laid down in this Regulation, including the preparation in the machine readable format that this Regulation provides for. Its date of application should therefore be deferred to 12 months following the date of entry into force. Persons drawing up the white papers should be required to publish the relevant white papers on their websites

in separate sections titled “white papers” by complying with the requirements laid down respectively in Articles 6, Article 19 and Article 51 of Regulation (EU) 2023/1114 and in Annexes I to III to the same Regulation for the period from [date of entry into force until 12 months after the date of entry into force.

- (12) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Securities and Markets Authority (‘ESMA’), in cooperation with the European Banking Authority.
- (13) ESMA has conducted open public consultations on the draft implementing 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<sup>84</sup>,

HAS ADOPTED THIS REGULATION:

### *Article 1*

#### **General principles for the presentation of the information**

1. Persons drawing up a crypto-asset white paper referred to in Articles 6(1), 19(1) or 51(1) of Regulation (EU) 2023/1114 shall provide the information required by this Regulation free of charge and in a manner that is non-discriminatory, fair, clear and not misleading, presented in a concise and comprehensible form and shall not omit material information.
2. Persons referred to in paragraph 1 shall lay out the information required by this Regulation in accordance with the templates set out in Table 2, Table 3 or Table 4 of Annex I, respectively for crypto-assets other than asset-referenced tokens or e-money tokens, asset-referenced tokens or e-money tokens.

### *Article 2*

#### **Format of the white paper**

1. Persons referred to in Article 1, paragraph 1, shall prepare the white paper in XHTML format and shall mark-up the fields prescribed in Annex I using the XBRL markup language.

---

<sup>84</sup> 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).

2. Persons referred to in Article 1, paragraph 1 shall embed the markups referred to in paragraph 1 in the white paper in XHTML format using the Inline XBRL 1.1 specifications and shall comply with the following requirements:
  - (a) submit the Inline XBRL instance document as a single XHTML file, and
  - (b) identify themselves in the Inline XBRL instance document using the ISO 17442 legal entity identifier or an equivalent identifier as specified in Article 14 of [RTS on record keeping] on the XBRL context entity identifiers and schemes.
3. Persons referred to in Article 1, paragraph 1, shall use a taxonomy in which the elements shall be those set out in Table 2, 3 or 4 of Annex I.

### *Article 3*

#### **Taxonomy files**

1. ESMA may publish machine-readable and downloadable XBRL taxonomy files based on the taxonomy referred to in Article 2 paragraph 3.

### *Article 4*

#### **Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from 12 months following date of entry into force.
3. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission  
The President

[For the Commission  
On behalf of the President

[Position]

ANNEX I

Table 1

**Legend for Tables 2, 3 and 4**

<b>SYMBOL</b>	<b>DATA TYPE</b>	<b>DEFINITION</b>
{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{CFI_CODE}	6 characters	ISO 10962 CFI code.
{COUNTRYCODE_2}	2 alphanumerical characters	2 letter country code, as defined by ISO 3166-1 alpha-2 country code
{CURRENCYCODE_3}	3 alphanumerical characters	3 letter currency code, as defined by ISO 4217 currency codes

{DATE _TIME_FORMAT}	ISO 8601 date and time format	Date and time in the following format: YYYY-MM-DDThh:mm:ss.dddZ. – ‘YYYY’ is the year; – ‘MM’ is the month; – ‘DD’ is the day; – ‘T’ – means that the letter ‘T’ shall be used – ‘hh’ is the hour; – ‘mm’ is the minute; – ‘ss.ddd’ is the second and its fraction of a second; – Z is UTC time. Dates and times shall be reported in UTC.
{DATEFORMAT}	ISO 8601 date format	Dates shall be formatted in the following way: YYYY-MM-DD.
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	Numerical field for both positive and negative values. – decimal separator is ‘.’ (full stop); – negative numbers are prefixed with ‘-’ (minus); Values are rounded and not truncated.
{DTI}	9 alphanumerical characters	Digital token identifier as defined in ISO 24165 standard



{DURATION}	3 characters	Represents a duration of time expressed as number of days.
{INTEGER-n}	Integer number of up to n digits in total	Numerical field for integer values.
{ISIN}	12 alphanumerical characters	ISIN code, as defined in ISO 6166 standard
{LEI}	20 alphanumerical characters	Legal entity identifier as defined in ISO 17442 standard
{MIC}	4 alphanumerical characters	Market identifier as defined in ISO 10383

Table 2

**Standard templates for white papers for crypto-assets other than asset-referenced tokens or e-money tokens**

N	FIELD	CONTENT TO BE REPORTED	FORM AND STANDARDS TO BE USED FOR REPORTING
00	Table of content	Table of content	Alphanumerical text
01	Date of notification	Date of notification	YYYY-MM-DD
02	Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	<p>'This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The offeror of the crypto-asset is solely responsible for the content of this crypto-asset white paper.'</p> <p>Where relevant in accordance with Article 6(3), second subparagraph of Regulation (EU) 2023/1114, reference shall be made to 'person seeking</p>	Predefined alphanumerical text

		admission to trading' or to 'operator of the trading platform' instead of 'offeror'.	
03	Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	'This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.'	Predefined alphanumerical text
04	Statement in accordance with Article 6(5), points (a), (b), (c) of Regulation (EU) 2023/1114	'The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.'	Predefined alphanumerical text
05	Statement in accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114	'The utility token referred to in this white paper may not be exchangeable against the good or service promised in the crypto-asset white paper, especially in the case of a failure or	'true' – Yes 'false' – Not applicable

		discontinuation of the crypto-asset project.’	If Yes, Predefined alphanumerical text
06	Statement in accordance with Article 6(5), points (e) and (f) of Regulation (EU) 2023/1114	<p>‘The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council.</p> <p>The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.’</p>	Predefined alphanumerical text
<i>SUMMARY</i>			
07	Warning in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114	<p>‘Warning</p> <p>This summary should be read as an introduction to the crypto-asset white paper.</p> <p>The prospective holder should base any decision to purchase this crypto – asset on the content of the crypto-asset white paper as a whole and not on the summary alone.</p> <p>The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial</p>	Predefined alphanumerical text

		<p>instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law.</p> <p>This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council (36) or any other offer document pursuant to Union or national law.'</p>	
08	Characteristics of the crypto-asset	A brief, clear and non-technical description of the characteristics of the crypto asset including information about rights and obligations of the purchaser, procedure and conditions for the exercise of those rights, conditions, if any, under which these rights and obligations may be modified.	Free alphanumerical text
09		Only applicable if field 08 is true. Information about the quality and quantity of goods or services to which	Free alphanumerical text

		the utility tokens give access and restrictions on the transferability.	
10	Key information about the offer to the public or admission to trading	<p>A brief and non-technical description of the offer to the public including information about the amount of the offer, including, where applicable, any minimum and maximum target subscription goals, issue price of the crypto-asset and subscription fees, the total number of crypto-assets to be offered; prospective holders; description, where applicable, of the various phases of the offer to the public of crypto-assets, including information on discounted purchase price for early purchasers of crypto-assets, subscription period.</p> <p>When applicable, the name of the crypto-asset service provider in charge of the placing of crypto-assets and the form of such placement (with or without a firm commitment basis);</p> <p>When applicable, a brief and non-technical description of the admission to trading, including the name of the</p>	Free alphanumerical text

		trading platform for which the admission is sought.	
<b>Part I – Information on risks</b>			
I.1	Offer-Related Risks	A description of the risks associated with the offer to the public of crypto-assets or their admission to trading	Free alphanumerical text
I.2	Issuer-Related Risks	A description of the risks associated with the issuer, if different from the offeror or person seeking admission to trading, including risks related to the issuer's financial situation, business activities and related sector, legal and regulatory risk, internal control risk, governance risks	Free alphanumerical text
I.3	Crypto-Assets-related Risks	A description of the risks associated with the crypto-assets	Free alphanumerical text
I.4	Project Implementation-Related Risks	A description of the risks associated with project implementation	Free alphanumerical text
I.5	Technology-Related Risks	A description of the risks associated with the technology used	Free alphanumerical text
I.6	Mitigation measures	Mitigation measures of the risks associated with the technology, if any	Free alphanumerical text
<i>Part A - Information about the offeror or the person seeking admission to trading</i>			
A.1	Name	Name	Free alphanumerical text

A.2	Legal form	Only applicable if an LEI is not provided in field A.6. Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'
A.3	Registered address	Only applicable if an LEI is not provided in field A.6. Address and country of registration	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text
A.4	Head office	Only applicable if an LEI is not provided in field A.6. Address and country of the Head office, where different than registered address	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text
A.5	Registration Date	Date of the registration	ISO 8601 date format (YYYY-MM-DD)
A.6	Legal entity identifier	Legal entity identifier of the offeror or person seeking admission to trading	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]



A.7	Another identifier required pursuant to applicable national law	<p>National identifier based on the nationality of the offeror or the person seeking admission to trading, if required under the applicable national law.</p> <p>This field only applies to entities for which a national identifier is required in accordance with applicable national law.</p>	Free text
A.8	Contact telephone number	Contact telephone number of the offeror or the person seeking admission to trading	Free alphanumerical text
A.9	E-mail address	E-mail address of the offeror or the person seeking admission to trading	Free alphanumerical text
A.10	Response Time (Days)	Period of days within which an investor will receive an answer via that telephone number or email address	{DURATION}
A.11	Parent Company	Field to be filled in only if an LEI is not provided in field A.6. Where applicable, the name of the parent company	Free alphanumerical text

A.12	Members of the Management body	Identity, business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the offeror or the person seeking admission to trading.	Free alphanumerical text presented in a tabular format
A.13	Business Activity	Business or professional activity of the offeror or person seeking admission to trading, including principal activities and principal markets	Free alphanumerical text
A.14	Parent Company Business Activity	Where applicable, business or professional activity of the parent company, including principal activities and principal markets	Free alphanumerical text
A.15	Newly Established	Indication as to whether the offeror or person seeking admission to trading has been established for the past three years	'true' – Yes 'false' – No
A.16	Financial condition for the past three years	Where the offeror or person seeking admission to trading has been established for the past three years,	Free alphanumerical text

		<p>the financial condition of the offeror or person seeking admission to trading over the past three years.</p> <p>This shall be assessed based on a fair review of the development and performance of the business of the offeror or person seeking admission to trading and of its position for each year and interim period for which historical financial information is required, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the business of the offeror or person seeking admission to trading and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the business.</p>	
--	--	--	--

		<p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (where available), information regarding unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.</p>	
A.17	Financial condition since registration	<p>Where the offeror or person seeking admission to trading has not been established for the past three years, description of its financial condition since the date of its registration.</p> <p>This shall be assessed based on a fair review of the development and</p>	Free alphanumerical text

		<p>performance of the business of the offeror or person seeking admission to trading and of its position for each year and interim period for which historical financial information is available, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the business of the offeror or person seeking admission to trading and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business.</p> <p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding</p>	
--	--	--	--

		unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.	
<i>Part B - Information about the issuer, if different from the offeror or person seeking admission to trading</i>			
B.1	Issuer different from offeror or person seeking admission to trading	Indication as to whether the issuer is different from the offeror or person seeking admission to trading	'true' – Yes 'false' – No
B.2	Name	Name	Free alphanumerical text
B.3	Legal form	Field to be filled in only if an LEI is not provided in field B.7.  Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'
B.4	Registered address	Field to be filled in only if an LEI is not provided in field B.7. Address and country of registration	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions

			and Free alphanumerical text
B.5	Head office	Field to be filled in only if an LEI is not provided in field B.7.  Address of the Head office, where different than registered address	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and Free alphanumerical text
B.6	Registration Date	Date of the registration	ISO 8601 date format (YYYY-MM-DD)
B.7	Legal entity identifier	Legal entity identifier of the issuer	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
B.8	Another identifier required pursuant to applicable national law	National identifier based on the nationality of the issuer, if required under the applicable national law.  This field only applies to entities for which a national identifier exists under applicable national law.	Free text

B.9	Parent Company	Field to be filled in only if an LEI is not provided in field B.7. Where applicable, the name of the parent company	Free alphanumerical text
B.10	Members of the Management body	Identity, business address and functions of each of the persons that are members of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the issuer.	Free alphanumerical text presented in a tabular format
B.11	Business Activity	Business or professional activity of the issuer, including principal activities, principal markets and recent financial condition.	Free alphanumerical text
B.12	Parent Company Business Activity	Where applicable, business or professional activity of the parent company, including principal activities and principal markets.	Free alphanumerical text



<i>Part C- Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114</i>			
C.1	Name	Name	Free alphanumerical text
C.2	Legal form	Field to be filled in only if an LEI is not provided in field C.6. Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'
C.3	Registered address	Field to be filled in only if an LEI is not provided in field C.6. Address of registration	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text
C.4	Head office	Field to be filled in only if an LEI is not provided in field C.6. Address of the Head office, where different than registered address	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text

C.5	Registration Date	Date of the registration	ISO 8601 date format (YYYY-MM-DD)
C.6	Legal entity identifier of the operator of the trading platform	Legal entity identifier of the operator of the trading platform	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
C.7	Another identifier required pursuant to applicable national law	National identifier based on the nationality of the issuer, if required under the applicable national law.  This field only applies to entities for which a national identifier is required under applicable national law.	Free text
C.8	Parent Company	Field to be filled in only if an LEI is not provided in field C.6. Where applicable, the name of the parent company	Free alphanumerical text
C.9	Reason for Crypto-Asset White Paper Preparation	The reason why the operator of the trading platform drew up the crypto-asset white paper	Free alphanumerical text

C.10	Members of the Management body	Identity (name or other identifiers), business address and functions of each of the persons that are members of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the operator of the trading platform.	Free alphanumerical text presented in a tabular format
C.11	Operator Business Activity	Business or professional activity of the operator, including principal activities and principal markets.	Free alphanumerical text
C.12	Parent Company Business Activity	Where applicable, business or professional activity of the parent company, including principal activities and principal markets.	Free alphanumerical text
C.13	Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	Where different from the offeror, person seeking admission to trading, issuer, operator of the trading platform, indication of the identity of the person drawing up the crypto-asset white paper	Free alphanumerical text

C.14	Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	Where the white paper is drawn up by a person different from the offeror, person seeking admission to trading, issuer, operator of the trading platform, reason for drawing up the white paper	Free alphanumerical text
<i>Part D- Information about the crypto-asset project</i>			
D.1	Crypto-asset project name	Name of the crypto-asset project, if different from the name of the offeror or person seeking admission to trading	Free alphanumerical text
D.2	Crypto-assets name	Field to be filled in only if a DTI is not provided in field F.14. Name of the crypto-assets, if different from the name of the offeror or person seeking admission to trading	Free alphanumerical text
D.3	Abbreviation	Field to be filled in only if a DTI is not provided in field F.12. Abbreviation or ticker handler	Free alphanumerical text

D.4	Crypto-asset project description	A brief description of the crypto-asset project	Free alphanumerical text
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	Details of advisors, development team, crypto-assets service providers and other persons involved in the implementation of the crypto-asset project, including business addresses or domicile of the company	Free alphanumerical text presented in a tabular format
D.6	Utility Token Classification	Indication as to whether the crypto-asset project concerns utility tokens	'true' – Yes 'false' – No
D.7	Key Features of Goods/Services for Utility Token Projects	Where applicable, key features of the goods or services to be developed for utility tokens crypto-asset projects	Free alphanumerical text
D.8	Plans for the token	Information about the crypto-asset project, including the description of the past and future milestones	Free alphanumerical text
D.9	Resource Allocation	Where applicable, information about resources, including financial resources, already allocated to the project	Free alphanumerical text

D.10	Planned Use of Collected Funds or Crypto-Assets	Where applicable, planned use of any funds or other crypto-assets collected	Free alphanumerical text
<i>Part E - Information about the offer to the public of crypto-assets or their admission to trading</i>			
E.1	Public Offering or Admission to trading	Indication as to whether the crypto-asset white paper concerns an offer to the public of crypto-assets or their admission to trading	'OTPC' - offer to the public  'ATTR' - admission to trading
E.2	Reasons for Public Offer or Admission to trading	The reasons for the offer to the public or for seeking admission to trading, including what is the intended use of the funds raised with the offer	Free alphanumerical text
E.3	Fundraising Target	Where applicable, the amount that the offer to the public intends to raise in funds or in any other crypto-asset in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3}  Or  Numerical {INTEGER-n}
E.4	Minimum Subscription Goals	Where applicable, any minimum target subscription goals set for the offer to the public of the crypto-assets	Amount in monetary value {DECIMAL-18/3}  or

		in an official currency or any other crypto-assets	Numerical {INTEGER-n}
E.5	Maximum Subscription Goal	Where applicable, any maximum target subscription goals set for the offer to the public of the crypto-assets in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3} or Numerical {INTEGER-n}
E.6	Oversubscription Acceptance	Indication whether oversubscriptions are accepted	'true'- Yes 'false' – No
E.7	Oversubscription Allocation	Where oversubscriptions are accepted, how they are allocated	Free alphanumerical text
E.8	Issue Price	The issue price of the crypto-asset being offered to the public in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3} Or Numerical {INTEGER-n}
E.9	Official currency or any other crypto-assets determining the issue price	The official currency or any other crypto-assets on the basis of which the issue price of the crypto asset is being offered to the public	{CURRENCYCODE_3} or {DTI}

E.10	Subscription fee	Any applicable subscription fee in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3}  Or  Numerical {INTEGER-n}
E.11	Offer Price Determination Method	Method in accordance with which the offer price will be determined	Free alphanumerical text
E.12	Total Number of Offered/Traded Crypto-Assets	Where applicable, the total number of crypto-assets to be offered to the public or admitted to trading	Numerical {INTEGER-n}
E.13	Targeted Holders	Indication of the prospective holders targeted by the offer to the public of the crypto-asset or admission of such crypto-asset to trading	'RETL' – retail investors  'PROF' – professional investors  'ALL' – all types of investors
E.14	Holder restrictions	Indication of any restriction as regards the type of holders for such crypto-asset	Free alphanumerical text



E.15	Reimbursement Notice	'Purchasers participating in the offer to this public of crypto-asset will be able to be reimbursed if the minimum target subscription goal is not reached at the end of the offer to the public, if they exercise the right to withdrawal foreseen in Article 13 of Regulation (EU) 2023/1114 or if the offer is cancelled'	Predefined alphanumerical text
E.16	Refund Mechanism	Detailed description of the refund mechanism	Free alphanumerical text
E.17	Refund Timeline	Expected timeline of when such refunds will be completed	Free alphanumerical text
E.18	Offer Phases	Information about the various phases of the offer to the public of the crypto-asset	Free alphanumerical text
E.19	Early Purchase Discount	Information on discounted purchase price for early purchasers of the crypto-asset - (pre-public sales) and in the case of discounted purchase price for some purchasers, an explanation as to why the purchase	Free alphanumerical text

		prices may be different and a description of the impact on the other investors	
E.20	Time-limited offer	Indication whether the offer is time-limited	'true'- Yes 'false' – No
E.21	Subscription period beginning	For time-limited offers, the beginning of the subscription period during which the offer to the public is open	ISO 8601 date format (YYYY-MM-DD)
E.22	Subscription period end	For time-limited offers, the end of the subscription period during which the offer to the public is open	ISO 8601 date format (YYYY-MM-DD)
E.23	Safeguarding Arrangements for Offered Funds/Crypto-Assets	The arrangements to safeguard funds or other crypto-assets as referred to in Article 10 of Regulation (EU) 2023/1114 during the time-limited offer to the public or during the withdrawal period	Free alphanumerical text
E.24	Payment Methods for Crypto-Asset Purchase	Methods of payment to purchase the crypto-assets	Free alphanumerical text

E.25	Value Transfer Methods for Reimbursement	Methods of transfer of the value to the purchasers when they are entitled to be reimbursed	Free alphanumerical text
E.26	Right of Withdrawal	In the case of offers to the public (field E1), information on the right of withdrawal as referred to in Article 13 of Regulation (EU) 2023/1114	Free alphanumerical text
E.27	Transfer of Purchased Crypto-Assets	Manner of transferring purchased crypto-assets to the holders	Free alphanumerical text
E.28	Transfer Time Schedule	Time schedule of transferring purchased crypto-assets to the holders	ISO 8601 date format (YYYY-MM-DD)
E.29	Purchaser's Technical Requirements	Information about technical requirements that the purchaser is required to fulfil to hold the crypto-assets	Free alphanumerical text
E.30	Crypto-asset service provider (CASP) name	Where applicable, the name of the crypto-asset service provider (CASP) in charge of the placing of crypto-assets	Free alphanumerical text

E.31	CASP identifier	Where available, the legal entity identifier of the crypto-asset service provider in charge of the placing of crypto-assets	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
E.32	Placement form	Where applicable, the form of such placement	'WITH- with a firm commitment basis 'WOUT' - without a firm commitment basis 'NTAV' - Not applicable
E.33	Trading Platforms name	Where applicable, the name of the trading platforms for crypto-assets where admission to trading is sought	Free alphanumerical text
E.34	Trading Platforms Market Identifier Code (MIC)	Segment MIC for the trading platform where the admission to trading of the crypto-assets is sought.	{MIC}
E.35	Trading Platforms Access	Where applicable, information about how investors can access such trading platforms	Free alphanumerical text
E.36	Involved costs	Where applicable, information about the costs involved in relation to the	Free alphanumerical text

		access of investors to the trading platforms	
E.37	Offer Expenses	Expenses related to the offer to the public of crypto-assets, in an official currency or any other crypto-assets	Free alphanumerical text and Amount in monetary value{DECIMAL-18/3}  [If more than one type of offer expense, expenses should be presented in a tabular format]
E.38	Conflicts of Interest	Potential conflicts of interest of the persons involved in the offer to the public or admission to trading, arising in relation to the offer or admission to trading	Free alphanumerical text
E.39	Applicable law	The law applicable to the offer to the public of the crypto-asset	Drop-down list of applicable laws
E.40	Competent court	Competent court	Free alphanumerical text
<i>Part F - Information about the crypto-assets</i>			

F.1	Crypto-Asset Type	The type of crypto-asset that will be offered to the public or for which admission to trading is sought	Free alphanumerical text
F.2	Crypto-Asset Functionality	A description of the functionality of the crypto-assets being offered or admitted to trading	Free alphanumerical text
F.3	Planned Application of Functionalities	Information about when the functionalities of the crypto-assets being offered or admitted to trading are planned to apply	Free alphanumerical text
<i>A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article</i>			
F.4	Type of white paper	The type of white paper notified.	OTHR
F.5	The type of submission	Type of submission	NEWT = New MODI = Modify EROR = Error CORR = Correction
F.6	Crypto-Asset Characteristics	A description of the characteristics of the crypto-asset	Free alphanumerical text

F.7	Commercial name or trading name	Field to be filled in only if a DTI is not provided in field F.14. Commercial name or trading name of the issuer.	Free alphanumerical text
F.8	Website of the issuer	Website of the issuer	Free alphanumerical text
F.9	Starting date of offer to the public or admission to trading	Starting date or, if not available at the time of the notification by the competent authority, the intended starting date of offer to the public or admission to trading.	YYYY-MM-DD
F.10	Publication date	Effective or intended publication date of the white paper or of the modified white paper	YYYY-MM-DD
F.11	Any other services provided by the issuer	Any other services provided by the issuer not covered by Regulation (EU) 2023/1114, with a reference to the applicable Union or national law.	Free alphanumerical text
F.12	Identifier of operator of the trading platform	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}

F.13	Language or languages of the white paper	Language or languages in which the crypto-asset white paper is drafted.  When multiple languages have been used, this field shall be reported as many times as necessary	Closed list of EU languages
F.14	Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	ISO 24165 Digital Token Identifier
F.15	Functionally Fungible Group Digital Token Identifier, where available	Code used to uniquely identify the functionally fungible group to which the digital asset belongs (i.e., common to each of the several assets to which the white paper relates, i.e. Code used to identify the white paper ISO 24165 DTI of type = 3 (i.e., functionally fungible group), where available	ISO 24165 FFG DTI
F.16	Voluntary data flag	Flag indicating the mandatory or voluntary nature of the white paper submitted in accordance with Article 4(8)	'true' – voluntary  'false' – mandatory



F.17	Personal data flag	Flag indicating if the submitted white paper contains personal data	'true' – Yes 'false' – No
F.18	LEI eligibility	Indication that the issuer is eligible for a Legal Entity Identifier .	'true' – eligible 'false' – not eligible
F.19	Home Member State	Home member state as defined in Article 3 paragraph 33 of Regulation (EU) 2023/1114	Closed list of EU member states
F.20	Host Member States	Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114.	Closed list of EU member states
<i>Part G - Information on the rights and obligations attached to the crypto-assets</i>			
G.1	Purchaser Rights and Obligations	A description of the rights and obligations, if any, of the purchaser	Free alphanumerical text
G.2	Exercise of Rights and obligations	Procedure and conditions for the exercise of rights	Free alphanumerical text
G.3	Conditions for modifications of rights and obligations	Description of the conditions under which the rights and obligations may be modified	Free alphanumerical text

G.4	Future Public Offers	Where applicable, information on the future offers to the public of crypto-assets by the issuer	Free alphanumerical text
G.5	Issuer Retained Crypto-Assets	Where applicable, information on the number of crypto-assets retained by the issuer itself	Numerical {INTEGER-n}
G.6	Utility Token Classification	Indication as to whether the offer to the public of crypto-assets or their admission to trading concerns utility tokens	'true' – Yes 'false' – No
G.7	Key Features of Goods/Services of Utility Tokens	Information about the quality and quantity of goods or services to which the utility tokens give access	Free alphanumerical text
G.8	Utility Tokens Redemption	Only applicable if field G.7 is true.  Information on how utility tokens can be redeemed for goods or services to which they relate	Free alphanumerical text
G.9	Non-Trading request	Indication as whether an admission to trading is sought	'true' – sought  'false' – not sought

G.10	Crypto-Assets purchase or sale modalities	Where an admission to trading is not sought, information on how and where the crypto-assets can be purchased or sold after the offer to the public	Free alphanumerical text
G.11	Crypto-Assets Transfer Restrictions	Restrictions on the transferability of the crypto-assets that are being offered or admitted to trading	Free alphanumerical text
G.12	Supply Adjustment Protocols	Indication as to whether the crypto-asset has protocols for the increase or decrease of their supply in response to changes in demand	'true' – Yes 'false' – No
G.13	Supply Adjustment Mechanisms	Where the crypto-assets has protocols for the increase or decrease of their supply in response to changes in demand, a description of the functioning of such protocols	Free alphanumerical text
G.14	Token Value Protection Schemes	Indication as to whether the crypto-asset has a protection scheme protecting the value of the crypto-asset	'true' – Yes 'false' – No

G.15	Token Value Protection Schemes Description	Where the field above is true, a description of the protection schemes protecting the value of the crypto-assets	Free alphanumerical text
G.16	Compensation Schemes	Indication as to whether the crypto-asset has a compensation schemes	'true' – Yes 'false' – No
G.17	Compensation Schemes Description	Where the field above is true, a description of the compensation schemes	Free alphanumerical text
G.18	Applicable law	The law applicable to the crypto-assets	Drop-down list of applicable laws
G.19	Competent court	Competent court	Free alphanumerical text
<i>Part H – information on the underlying technology</i>			
H.1	Distributed ledger technology	Field to be filled in only if a DTI is not provided in field F.14. Information on the technology used, including distributed ledger technology	Free alphanumerical text

H.2	Protocols and technical standards	Information about protocols and technical standards used	Free alphanumerical text
H.3	Technology Used	Other information on the technology used allowing for the holding, storing and transfer of crypto-assets, if relevant	Free alphanumerical text
H.4	Consensus Mechanism	Information on the consensus mechanism, where applicable	Free alphanumerical text
H.5	Incentive Mechanisms and Applicable Fees	Information on incentive mechanisms to secure transactions and any fees applicable	Free alphanumerical text
H.6	Use of Distributed Ledger Technology	Indication as to whether the crypto-assets are issued, transferred and stored using distributed ledger technology that is operated by the issuer, the offeror or a third-party acting on their behalf	<p>'true' – Yes, DLT operated by the issuer or a third-party acting on the issuer's behalf</p> <p>'false' – No, DLT not operated by the issuer or a third-party acting on the issuer's behalf</p>
H.7	DLT Functionality Description	If the DLT is operated by the issuer or a third party acting on the issuer's behalf, a detailed description of the	Free alphanumerical text

		functioning of such distributed ledger technology	
H.8	Audit	Indication as to whether an audit of the technology used was conducted	'true' – Yes 'false' – No
H.9	Audit outcome	If an audit was conducted, information on the outcome of the audit of the technology used	Free alphanumerical text
J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts			
J-1	Adverse impacts on climate and other environment-related adverse impacts	Information referred to in the Annex to Commission Delegated Regulation (XX) [Delegated Regulation (EU) 2024/XXX specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts]	Free alphanumerical text

*Table 3*

**Disclosure template for white papers for asset-referenced tokens**

<b>N</b>	<b>FIELD</b>	<b>CONTENT TO BE REPORTED</b>	<b>FORM AND STANDARDS</b>
I.	Table of content	Table of content	alphanumerical text
I.	Date of notification	Date of notification	YYYY-MM-DD
I.	Statement in accordance with Article Art.19(4), points (a), (b), (c), (d) and (e) of Regulation (EU) 2023/1114	'The asset-referenced token referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.	Predefined alphanumerical text

		<p>The asset-referenced token referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC.</p> <p>The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU.'</p>	
I.	Compliance statement in accordance with Article 19(5) of Regulation (EU) 2023/1114	'This crypto-asset white paper complies with Title III of Regulation (EU) 2023/1114 and to the best of the knowledge of the management body, the information presented in this crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.'	Predefined alphanumeric text
<i>SUMMARY</i>			
I.04	Warning in accordance with Article 19(6), second subparagraph, of Regulation (EU) 2023/1114	<p style="text-align: center;">'Warning</p> <p>This summary should be read as an introduction to the crypto-asset white paper.</p> <p>The prospective holder should base any decision to purchase this asset-referenced token on the content of the crypto-asset white paper as a whole and not on the summary alone.</p> <p>The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and that any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law.</p> <p>This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament</p>	Predefined alphanumeric text



		and of the Council (36) or any other offer document pursuant to Union or national law.'	
I.05	Characteristics of the crypto-asset	A brief, clear and non-technical description of the characteristics of the asset-referenced token concerned in order to help prospective holders of that asset-referenced token make an informed decision	Free alphanumerical text
I.06	Right of redemption	'The holders of asset-referenced tokens have a right of redemption at any time'  Description of the conditions for such redemption.	Predefined alphanumerical text  Free alphanumerical text
I.07	Key information about the offer to the public and or admission to trading	Key information about the offer to the public of the asset-referenced token or the intended admission to trading of the asset-referenced token.	Free alphanumerical text
<i>Part F - Information on the risks</i>			

F.1	Risks related to Asset Reserve	The risks related to the reserve of assets, when the issuer is not able to fulfil its obligations	Free alphanumerical text
F.2	Issuer-Related Risks	A description of the risks associated with the issuer of the asset-referenced token, including risks related to the issuer's financial situation, risks related to the issuer's business activities and industry, legal and regulatory risk, governance and internal control risk	Free alphanumerical text
F.3	Offer-Related Risks	A description of the risks associated with the offer to the public of the asset-referenced token or its admission to trading	Free alphanumerical text
F.4	Token-Related Risks	Description of the risks associated with the asset-referenced token, in particular with regard to the asset referenced and environmental risks	Free alphanumerical text
F.5	Risks related to operationalisation of the Asset-Referenced Token Project	A description of the risks associated with the operationalisation of the asset-referenced token project	Free alphanumerical text

F.6	Technology-Related Risks	Description of the risks associated with the technology used	Free alphanumerical text
F.7	Mitigation measures	Mitigation measures of the risks associated with the technology used, if any	Free alphanumerical text
<i>Part A – Information about the issuer of the asset-referenced token</i>			
A.1	Statutory Name	Statutory Name	Free alphanumerical text
A.2	Trading Name	Trading Name	Free alphanumerical text
A.3	Legal form	Field to be filled in only if an LEI is not provided in field A.7. Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'
A.4	Registered address	Field to be filled in only if an LEI is not provided in field A.7. Address and country of registration	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text

A.5	Head office	Field to be filled in only if an LEI is not provided in field A.7. Address and country of the Head office, where different than registered address	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text
A.6	Registration Date	Date of the registration	ISO 8601 date format (YYYY-MM-DD)
A.7	Legal entity identifier	Legal entity identifier of the issuer	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
A.8	Other identifier required pursuant to applicable national law	National identifier based on the nationality of the issuer, if required under the applicable national law.  This field only applies to entities for which a national identifier exists under applicable national law.	Free text
A.9	Parent Company	Field to be filled in only if an LEI is not provided in field A.7. Where applicable, the identity name of the parent company	Free alphanumerical text
A.10	Members of the Management body	Identity, business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the issuer	Free alphanumerical text presented in a tabular format

A.11	Business Activity	Business or professional activity of the issuer, including principal activities and principal markets	Free alphanumerical text
A.12	Parent Company Business Activity	Business or professional activity of the parent company (if applicable), including principal activities and principal markets	Free alphanumerical text
A.13	Newly Established	Indication as to whether the issuer has been established for the past three years	'true' – Yes 'false' – No
A.14	Financial condition for the past three years	<p>Financial condition of the issuer over the past three years.</p> <p>This shall be assessed based on a fair review of the development and performance of the business of the issuer and of its position for each year and interim period for which historical financial information is required, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the business of the issuer and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business.</p> <p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding unusual or</p>	Free alphanumerical text

		infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.	
A.15	Financial condition since registration	<p>Where the issuer has not been established for the past three years, its financial condition since the date of its registration.</p> <p>This shall be assessed based on a fair review of the development and performance of the business of the issuer and of its position for each year and interim period for which historical financial information is required, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the business of the issuer and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business.</p> <p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding unusual or</p>	Free alphanumerical text

		infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.	
A.16	Governance Arrangements	A detailed description of the issuer's governance arrangements	Free alphanumerical text
A.17	Exemption from authorisation	Indication of whether the issuer of asset-referenced tokens is exempted from authorisation	'NOEX' – No exemption 'EX17' – Exemption in accordance with Article 17 'EX16' – Exemption in accordance with Article 16
A.18	Authorisation as issuer of Asset-referenced Token	If not exempted from authorisation, details about the authorisation as an issuer of an asset-referenced token	Free alphanumerical text
A.19	Authorisation Authority	Name of the competent authority that granted the authorisation as issuer of asset-referenced tokens	Closed list of competent authorities – one per Member State

A.20	Competent Authority for credit institutions	For credit institutions, name of the competent authority of the home Member State	Closed list of competent authorities – one per Member State
A.21	Issuance of other crypto-assets	Indication of whether the issuer of the asset-referenced token also issues other crypto-assets	'true' – Yes 'false' – No
A.22	Activities related to other crypto-assets	Indication of whether the issuer of the asset-referenced token also has activities related to other crypto-assets.	'true' – Yes 'false' – No
A.23	Connection between the issuer and the entity running the DLT	Indication of whether there is any connection between the issuer and the entity running the distributed ledger technology used to issue the crypto-asset, including if the protocols are run or controlled by a person closely connected to the project participants	'true' – Yes 'false' – No
A.24	Description of the connection between the issuer and the entity running the DLT	Description of the connection between the issuer and entity running the distributed ledger technology used to issue the crypto-asset, including if the protocols are run or controlled by a person closely connected to the project participants	Free alphanumerical text



AA- information on other persons offering to the public or seeking admission to trading of asset-referenced tokens other than the issuer and on other persons drawing up the crypto-asset white paper according to Article 19(1), second subparagraph, of Regulation (EU) 2023/1114			
AA .1	Persons other than the issuer offering to the public or seeking admission to trading of the asset referenced token according to Article 19(1), second subparagraph, of Regulation (EU) 2023/1114	Where different from the issuer, indication of the identity of the person offering to the public or seeking admission to trading of the asset referenced token	{LEI} or different identifier as specified in Article 14 of [RTS on record keeping]
AA .2	Reason for offering to the public or seeking admission to trading the asset-referenced token by persons referred to in Article 19(1), second subparagraph, of Regulation (EU) 2023/1114	Where the offeror or the person seeking admission to trading is different from the issuer, reason for offering to the public or seeking admission to trading of the asset-referenced token	Free alphanumerical text
AA .3	Other persons drawing up the crypto-asset white paper according to Article 19(1), second subparagraph, of Regulation (EU) 2023/1114	Where different from the issuer, indication of the identity of the person drawing up the crypto-asset white paper	{LEI} or different identifier as specified in Article 14 of [RTS on record keeping]

AA .4	Reason for drawing the white paper by persons referred to in Article 19(1), second subparagraph, of Regulation (EU) 2023/1114	Where the white paper is drawn up by a person different from the issuer, reason for drawing up the white paper	Free alphanumerical text
<i>Part B - Information about the asset-referenced token</i>			
B.1	Asset-referenced Token Name	Field to be filled in only if a DTI is not provided in field B.17. Name of the asset-referenced token	Free alphanumerical text
B.2	Token Abbreviation	Field to be filled in only if a DTI is not provided in field B.17. Abbreviation or ticker handler of the asset-referenced token	Free alphanumerical text
B.3	Details of all natural or legal persons involved in the operationalisation of the asset-referenced token	Details of advisors, development team, CASPs and all other natural or legal persons involved in the implementation of the crypto-asset project, including business addresses or domicile of the company	Free alphanumerical text presented in a tabular format
B.4	Third-Party Roles	A description of the role, responsibility and accountability of any third-party entities referred to in Article 34(5), first subparagraph, point (h) of Regulation (EU) 2023/1114	Free alphanumerical text presented in a tabular format
B.5	Plans for the Token	Information about the plans for the asset-referenced tokens, including description of past and expected future milestones	Free alphanumerical text

B.6	Resource Allocation	Where applicable, information about resources already allocated to the project	Free alphanumerical text
<i>A description of the characteristics of the asset referenced token, including the data necessary for classification of the white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article</i>			
B.7	Type of white paper	The type of white paper notified. .	ARTW
B.8	The type of submission	Type of submission	NEWT = New MODI = Modify EROR = Error CORR = Correction
B.9	Crypto-Asset Characteristics	A description of the characteristics of the asset referenced token being offered or admitted to trading	Free alphanumerical text
B.10	Website of the issuer	Website of the issuer	Free alphanumerical text
B.11	Starting date of offer to the public or admission to trading	Starting date or, if not available at the time of the notification by the competent authority, the intended starting date of offer to the public or admission to trading.	YYYY-MM-DD

B.12	Publication date	Effective or intended publication date of the white paper or of the modified white paper	YYYY-MM-DD
B.13	Any other services provided by the issuer	Any other services provided by the issuer not covered by Regulation (EU) 2023/1114, with a reference to the applicable Union or national law.	Free alphanumerical text
B.14	Identifier of operator of the trading platform	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}
B.15	Language or languages of the white paper	Language or languages in which the crypto-asset white paper is drafted.  When multiple languages have been used, this field shall be reported as many times as necessary	Closed list of EU languages
B.16	Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	ISO 24165 Digital Token Identifier
B.17	Functionally Fungible Group Digital Token Identifier, where available	Code used to uniquely identify the functionally fungible group to which the digital asset belongs (i.e., common to each of the several assets to which the white paper relates, i.e. Code used to identify the white paper ISO 24165 DTI of type = 3 (i.e., functionally fungible group), where available	ISO 24165 FFG DTI

B.18	Personal data flag	Flag indicating if the submitted white paper contains personal data	'true' – Yes  'false' – No
B.19	LEI eligibility	Indication that the issuer is eligible for a Legal Entity Identifier .	'true' – eligible  'false' – not eligible
B.20	Home Member State	Home member state as defined in Article 3 paragraph 33 of Regulation (EU) 2023/1114	Closed list of EU member states
B.21	Host Member States	Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114.	Closed list of EU member states
<i>Part C - Information about the offer to the public of the asset-referenced token or its admission to trading</i>			
C.1	Public Offering or admission to trading	Indication as to whether the crypto-asset white paper concerns an offer to the public of the asset-referenced token or its admission to trading	'OTPC' - offer to the public  'ATTR' - admission to trading
C.2	Fundraising Target	Where applicable, the amount that the offer to the public of the asset-referenced token intends to raise in funds in an official currency or in any other crypto-asset	Amount in monetary value {DECIMAL-18/3}  or  Numerical {INTEGER-n}

C.3	Minimum Subscription Goals	Where applicable, any minimum target subscription goals set for the offer to the public of the asset-referenced token in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3} or Numerical {INTEGER-n}
C.4	Maximum Subscription Goals	Where applicable, any maximum target subscription goals set for the offer to the public of the asset-referenced token in an official currency or any other crypto-assets	Amount in monetary value {DECIMAL-18/3} or Numerical {INTEGER-n}
C.5	Oversubscription Acceptance	Indication whether oversubscriptions are accepted	'true' - Yes 'false' - No 'NTAV' - Not applicable
C.6	Oversubscription Allocation	Where oversubscriptions are accepted, description of how they are allocated	Free alphanumerical text
C.7	Token Offering/Trading Quantity	Where applicable, the total number of units of the asset-referenced token to be offered or admitted to trading	Numerical {DECIMAL-18/3}

C.8	Targeted Holders	Indication of the prospective holders targeted by the offer to the public of the asset-referenced token or admission of such asset-referenced token to trading	'RETL' – retail investors  'PROF' – professional investors
C.9	Holder restrictions	Indication of any restriction as regards the type of holders for such asset-referenced token	Free alphanumerical text
C.10	Reimbursement Notice	'Purchasers participating in the offer to the public of this asset-referenced token will be able to be reimbursed if the minimum target subscription goal is not reached at the end of the offer to the public, if they exercise the right to withdrawal foreseen in Article 13 of Regulation (EU) 2023/1114 or if the offer is cancelled'	Predefined alphanumerical text
C.11	Refund Timeline	Expected timeline of when such refunds will be completed	Free alphanumerical text
C.12	Explicit consequences	Description of the consequences of exceeding a maximum target subscription goal	Free alphanumerical text
C.13	Offer Phases	Information about the various phases of the offer to the public of the asset-referenced token	Free alphanumerical text
C.14	Early Purchase Discount	Information on discounted purchase price for early purchasers of the asset-referenced token (pre-public sales) and in the case of discounted purchase price for some purchasers, an explanation as to	Free alphanumerical text

		why the purchase prices may be different and a description of the impact on the other investors	
C.15	Time-limited offer	Indication whether the offer is time-limited	'true'- Yes 'false' – No
C.16	Subscription period beginning	For time-limited offers, the beginning of the subscription period during which the offer to the public is open	ISO 8601 date format (YYYY-MM-DD)
C.17	Subscription period end	For time-limited offers, the end of the subscription period during which the offer to the public is open	ISO 8601 date format (YYYY-MM-DD)
C.18	Token Purchase/Redemption Payment	Methods of payment to purchase and to redeem the asset-referenced token offered	Free alphanumerical text
C.19	Token Transfer	Information on the method and time schedule of transferring the purchased asset-referenced token to the holders	Free alphanumerical text
C.20	Purchasers technical requirements	Information about technical requirements that the purchaser is required to fulfil to hold the asset-referenced token	Free alphanumerical text
C.21	CASP name	Where applicable, the name of the crypto-asset service provider in charge of the placing of asset-referenced tokens	Free alphanumerical text



C.22	CASP identifier	Where available, the legal entity identifier of the crypto-asset service provider in charge of the placing of asset-referenced tokens	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
C.23	Placement form	Where applicable, the form of such placement (with or without a firm commitment basis)	'WITH- with a firm commitment basis  'WOUT' - without a firm commitment basis  'NTAV' - Not applicable
C.24	Trading Platforms name	Where applicable, the name of the trading platforms for crypto-assets where admission to trading is sought	Free alphanumerical text
C.25	Trading Platforms Market Identifier Code (MIC)	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}
C.26	Trading Platforms Access	Where applicable, information about how investors can access such trading platforms	Free alphanumerical text
C.27	Involved costs	Where applicable, information about the costs involved for accessing the trading platform for investors	Free alphanumerical text

C.28	Offer Expenses	Expenses related to the offer to the public of the asset-referenced token, in an official currency or any other crypto-assets. If more than one type of expense, expenses should be presented in a tabular format.	Free alphanumerical text and Numerical {DECIMAL-18/3} presented in tabular format
C.29	Conflicts of Interest	Potential conflicts of interest of the persons involved in the offer to the public or admission to trading, arising in relation to the offer or admission to trading	Free alphanumerical text
C.30	Applicable law	The law applicable to the offer to the public of the asset-referenced token	Drop-down list of applicable laws
C.31	Competent court	Competent court	Free alphanumerical text
<i>Part D - Information on the rights and obligations attached to the asset-referenced token</i>			
D.1	Token Functionalities	A description of the functionality of the asset-referenced token being offered or admitted to trading	Free alphanumerical text
D.2	Planned Functional Use	Information about when the functionalities are planned to apply	ISO 8601 date format(YYYY-MM-DD)
D.3	Purchaser Rights & Obligations	A description of the rights and obligations, if any, of the purchaser	Free alphanumerical text
D.4	Rights Exercise Procedure	A description of the procedure and conditions for the exercise of those rights	Free alphanumerical text

D.5	Conditions for modifications of rights and obligations	A description of the conditions under which the rights and obligations may be modified	Free alphanumerical text
D.6	Future Public Offers	Where applicable, information on the future offers to the public of the asset-referenced token by the issuer	Free alphanumerical text
D.7	Issuer Retained Units	Where applicable, information on the number of units of the asset-referenced token retained by the issuer itself	Numerical {INTEGER-n}
D.8	Non-Trading Request	Indication as to whether an admission to trading is sought	'true' –sought 'false' – not sought
D.9	Token purchase or sale modalities	Where an admission to trading is not sought, information on how and where the asset-referenced token can be purchased or sold after the offer to the public	Free alphanumerical text
D.10	Token Transfer Restrictions	Any restrictions on the transferability of the asset-referenced token that is being offered or admitted to trading	Free alphanumerical text
D.11	Supply Adjustment Protocols	Indication as to whether the asset-referenced token has protocols for the increase or decrease of their supply in response to changes in demand	'true' – Yes 'false' – No
D.12	Supply Adjustment Mechanisms	Where the asset-referenced token has protocols for the increase or decrease of their supply in response to changes in demand, a description of the functioning of such protocols	Free alphanumerical text

D.13	Token Value Protection Schemes	Indication as to whether the asset-referenced token has a protection schemes protecting the value of the asset-referenced token	'true' – Yes  'false' – No
D.14	Token Value Protection Schemes Description	Where yes in the field above, a description of the protection schemes protecting the value of the asset-referenced token	Free alphanumerical text
D.15	Compensation Schemes	Indication as to whether the asset-referenced token has a compensation schemes	'true' – Yes  'false' – No
D.16	Compensation Schemes Description	Where yes in the field above, a description of compensation schemes	Free alphanumerical text
D.17	Nature and enforceability of rights	Information on the nature and enforceability of rights, including permanent rights of redemption and any claims that holders and any legal or natural person as referred to in Article 39(2) of Regulation (EU) 2023/1114, may have against the issuer, including information on how such rights will be treated in the case of insolvency procedures and whether different rights are allocated to different holders and the non-discriminatory reasons for such different treatment	Free alphanumerical text
D.18	Referenced assets description	Detailed description of the claim that the asset-referenced token represents for holders, including a description of each referenced asset including the ISIN code where available and specified proportions of each of those assets	Free alphanumerical text presented in a tabular format  {ISIN} where applicable

D.19	Referenced assets proportions	Description of the amount of the claim and the reserve of asset	Free alphanumerical text
D.20	Value-Claim-Reserve Interrelation	Relation between the value of the referenced assets and the amount of the claim and the reserve of assets	Free alphanumerical text
D.21	Transparent Claim Valuation	Description how a fair and transparent valuation of components of the claim is undertaken, which identifies, where relevant, independent parties	Free alphanumerical text
D.22	Other details about the claim the asset referenced token represents over referenced assets	Additional details describing the claim that the asset-referenced token represents for the holders	Free alphanumerical text
D.23	Liquidity Arrangements	Where applicable, information on the arrangements put in place by the issuer to ensure the liquidity of the asset-referenced token	Free alphanumerical text
D.24	Liquidity Providers	Where applicable, the name of the entities in charge of ensuring such liquidity	Free alphanumerical text
D.25	Complaint Submission Contact	Contact details for submitting complaints	Free alphanumerical text
D.26	Complaints Handling Procedures	Description of the complaints-handling procedures	Free alphanumerical text
D.27	Dispute Resolution Mechanism	Description of any dispute resolution mechanism or redress procedure established by the issuer of the asset-referenced token	Free alphanumerical text

D.28	Holder Rights in Default or Insolvency	A description of the rights of the holders when the issuer is not able to fulfil its obligations, including in insolvency	Free alphanumerical text
D.29	Rights in Recovery Plan Implementation	A description of the rights in the context of the implementation of the recovery plan	Free alphanumerical text
D.30	Rights in Redemption Plan Implementation	A description of the rights in the context of the implementation of the redemption plan	Free alphanumerical text
D.31	Redemption Form	Detailed information on how the asset-referenced token is redeemed	Free alphanumerical text
D.32	Redemption Form Options	Indication whether the holder will be able to choose the form of redemption	'true' – Yes 'false' – No
D.33	Transference Form Options	Indication as to whether the holder will be able to choose the form of transference	'true' – Yes 'false' – No
D.34	Form of transference	Form of transference	Free alphanumerical text
D.35	Redemption Currency	The official currency of redemption	{CURRENCYCODE_3}
D.36	Applicable law	The law applicable to the asset-referenced token	Drop-down list of applicable laws
D.37	Competent court	Competent court	Free alphanumerical text

<i>Part E - Information on the underlying technology</i>			
E.1	Distributed ledger technology	Fill in the field only if a DTI is not provided in field B.17. Information on the distributed ledger technology	Free alphanumerical text
E.2	Protocols and technical standards	Information on the protocols and technical standards used, allowing for the holding, storing and transfer of the asset-referenced token	Free alphanumerical text
E.3	Technology Used	Other information on the technology used allowing for the holding, storing and transfer of asset-referenced tokens, if relevant	Free alphanumerical text
E.4	Consensus Mechanism	The consensus mechanism, where applicable	Free alphanumerical text
E.5	Incentive Mechanisms and Applicable Fees	Incentive mechanisms to secure transactions and any fees applicable	Free alphanumerical text
E.6	Use of Distributed Ledger Technology	Indication as to whether the asset-referenced token are issued, transferred and stored using distributed ledger technology that is operated by the issuer or a third-party acting on the issuer's behalf	'true' – Yes, DLT operated by the issuer or a third-party acting on the issuer's behalf 'false' – No, DLT not operated by the issuer or a third-party acting on the issuer's behalf

E.7	DLT Functionality Description	If the DLT is operated by the issuer or a third party acting on the issuer's behalf, a detailed description of the functioning of such distributed ledger technology	Free alphanumerical text
E.8	Audit	Indication as to whether an audit of the technology used was conducted	'true' – Yes 'false' – No
E.9	Audit outcome	If an audit was conducted, information on the outcome of the audit of the technology used	Free alphanumerical text
<i>Part G - Information on the reserve of assets</i>			
G.1	Value Alignment Mechanism	Detailed description of the mechanism aimed at aligning the value of the reserve of assets with the claim associated with the asset-referenced token, including legal and technical aspects	Free alphanumerical text
G.2	Asset Reserve Description	Detailed description of the reserve of assets and their composition	Free alphanumerical text
G.3	Token Issuance and Redemption Mechanisms	A description of the mechanisms through which asset-referenced tokens are issued and redeemed	Free alphanumerical text
G.4	Investment of Reserve of Assets	Information on whether a part of the reserve assets are invested	'true' – Yes 'false' – No
G.5	Reserve Asset Investment Policy	If a part of the reserve assets are invested, a description of the investment policy for the reserve assets	Free alphanumerical text



G.6	Reserve Asset Custody Arrangements	Description of the custody arrangements for the reserve assets, including their segregation	Free alphanumerical text
G.7	Custodian Service Providers	Name of crypto-asset service providers providing custody and administration of crypto-assets on behalf of clients, credit institutions, or investment firms appointed as custodians of the reserve assets	Free alphanumerical text
G.8	Custodian Service Providers	LEI of the CASP providing custody and administration of crypto-assets on behalf of clients, credit institutions, or investment firms appointed as custodians of the reserve assets	{LEI} or different identifier as specified in Article 14 of [ <i>Delegated Regulation (EU) xx/xxx RTS on record keeping</i> ]
<i>H – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts</i>			
H-1	Adverse impacts on climate and other environment-related adverse impacts	Include the information referred to in the Annex to Commission Delegated Regulation (XX) [Commission Delegated Regulation (EU) 2024/XXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts]	Free alphanumerical text

Table 4

**Disclosure template for white papers for e-money tokens**

<b>N</b>	<b>FIELD</b>	<b>CONTENT TO BE REPORTED</b>	<b>FORM AND STANDARDS TO BE USED FOR REPORTING</b>
I.00	Table of content	Table of content	Alphanumerical text
I.01	Date of notification	Date of notification	YYYY-MM-DD
I.02	Statement in accordance with Article 51(3) of Regulation (EU) 2023/1114	'This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The issuer of the crypto-asset is solely responsible for the content of this crypto-asset white paper.'	Predefined alphanumerical text
I.03	Compliance statement in accordance with Article 51(5) of	'This crypto-asset white paper complies with Title IV of Regulation (EU) 2023/1114 and to the best of the knowledge of the management body, the information presented in this crypto-asset white paper is fair, clear and	Predefined alphanumerical text

	Regulation (EU) 2023/1114	not misleading and the crypto-asset white paper makes no omission likely to affect its import.'	
I.04	Warning in accordance with Article 51(4), points (a) and (b) of Regulation (EU) 2023/1114	'This e-money token is not covered by the investor compensation schemes under Directive 97/9/EC. This e-money token is not covered by the deposit guarantee schemes under Directive 2014/49/EU.'	Predefined alphanumerical text
<i>SUMMARY</i>			
I.05	Warning in accordance with Article 51(6), second subparagraph of Regulation (EU) 2023/1114s	<p style="text-align: center;">Warning</p> <p>This summary should be read as an introduction to the crypto-asset white paper.</p> <p>The prospective holder should base any decision to purchase this e-money token on the content of the crypto-asset white paper as a whole and not on the summary alone.</p> <p>The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and that any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law.</p> <p>This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council (36) or any other offer document pursuant to Union or national law.'</p>	Predefined alphanumerical text

I.06	Characteristics of the crypto-asset	A brief, clear and non-technical description of the characteristics of the crypto-assets concerned in order to help prospective holders of the crypto-asset make an informed decision	Free alphanumerical text
I.07	Right of redemption	<p>'The holders of this e-money token have a right of redemption at any time and at par value.'</p> <p>Description of the conditions for such redemption.</p>	<p>Predefined alphanumerical text</p> <p>Free alphanumerical text</p>
I.08	Key information about the offer and/ or admission to trading	Key information about the offer to the public of the e-money token or the intended admission to trading of such e-money token.	Free alphanumerical text
<i>Part F - Information on the risks</i>			
F.1	Issuer-Related Risks	A description of the risks associated with the issuer of the e-money token, including: risks related to the issuer's financial situation, risks related to the issuer's business activities and industry, legal and regulatory risk, internal control risk	Free alphanumerical text
F.2	Token-Related Risks	A description of the risks associated with the e-money token	Free alphanumerical text

F.3	Technology-Related Risks	Description of the risks associated with the technology used	Free alphanumerical text
F.4	Mitigation measures	Mitigation measures of the risks associated with the technology used, if any	Free alphanumerical text
<i>Part A - Information about the issuer of the e-money token</i>			
A.1	Statutory Name	Statutory Name	Free alphanumerical text
A.2	Trading Name	Trading Name	Free alphanumerical text
A.3	Legal form	Fill in the field only if an LEI is not provided in field A.7. Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'
A.4	Registered address	Fill in the field only if an LEI is not provided in field A.7. Address and country of registration	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and  Free alphanumerical text
A.5	Head office	Fill in the field only if an LEI is not provided in field A.7. Address and country of the Head office, where different than registered address	ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions  and

			Free alphanumerical text
A.6	Registration Date	Date of the registration	ISO 8601 date format (YYYY-MM-DD)
A.7	Legal entity identifier	Legal entity identifier of the issuer	{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]
A.8	Another identifier required pursuant to applicable law	National identifier based on the nationality of the issuer, if required under the applicable national law.  This field only applies to entities for which a national identifier exists under applicable national law.	Free text
A.9	Contact telephone number	Contact telephone number of the issuer	Free alphanumerical text
A.10	E-mail address	E-mail address of the issuer	Free alphanumerical text
A.11	Response Time (Days)	Period of days within which an investor via that telephone number or email address will receive an answer	{DURATION}
A.12	Parent Company	Fill in the field only if an LEI is not provided in field A.7. Where applicable, the name of the parent company	Free alphanumerical text

A.13	Members of the management body	Identity, business address and functions of persons (names or other identifiers) within the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the issuer.	Free alphanumerical text presented in a tabular format
A.14	Business Activity	Business or professional activity of the issuer, including principal activities and principal markets	Free alphanumerical text
A.15	Parent Company Business Activity	Business or professional activity of the parent company (if applicable), including principal activities and principal markets	Free alphanumerical text
A.16	Conflicts of Interest Disclosure	Potential conflicts of interest	Free alphanumerical text
A.17	Issuance of other crypto-assets	Indication of whether the issuer of the e-money token also issues other crypto-assets	'true' – Yes 'false' – No
A.18	Activities related to other crypto-assets	Indication of whether the issuer of the e-money token also has activities related to other crypto-assets.	'true' – Yes 'false' – No

A.19	Connection between the issuer and the entity running the DLT	Indication of whether there is any connection between the issuer and the entity running the distributed ledger technology used to issue the crypto-asset, including if the protocols are run or controlled by a person closely connected to the project participants	'true' – Yes 'false' – No
A.20	Description of the connection between the issuer and the entity running the DLT	Description of the connection between the issuer and entity running the distributed ledger technology used to issue the crypto-asset, including if the protocols are run or controlled by a person closely connected to the project participants	Free alphanumerical text
A.21	Newly Established	Indication as to whether the issuer has been established for the past three years	'true' – Yes 'false' – No
A.22	Financial condition for the past three years	<p>Financial condition of the issuer over the past three years.</p> <p>This shall be assessed based on a fair review of the development and performance of the business of the issuer and of its position for each year and interim period for which historical financial information is required, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the</p>	Free alphanumerical text



		<p>business of the issuer and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business.</p> <p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.</p>	
A.23	Financial condition since registration	<p>Where the issuer has not been established for the past three years, its financial condition since the date of its registration.</p> <p>This shall be assessed based on a fair review of the development and performance of the business of the issuer and of its position for each year and interim period</p>	Free alphanumerical text

		<p>for which historical financial information is required, including the causes of material changes.</p> <p>The review shall be a balanced and comprehensive analysis of the development and performance of the business of the issuer and of its position, consistent with the size and complexity of the business.</p> <p>The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business.</p> <p>The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.</p>	
A.24	Exemption from authorisation	Indication of whether the issuer of e-money token is exempted from authorisation in accordance with Article 48(4) and (5) of Regulation (EU) 2023/1114	'true' – Yes 'false' – No

A.25	E-money Token Authorisation	If not exempted from authorisation in accordance with Article 48(4) and (5) of Regulation (EU) 2023/1114, details about the authorisation as an issuer of an e-money token	Free alphanumerical text
A.26	Authorisation Authority	Name of the competent authority that granted the authorisation	Closed list of competent authorities – one per Member State
A.27	Persons other than the issuer offering to the public or seeking admission to trading of the e-money token according to Article 51(1), second subparagraph, of Regulation (EU) 2023/1114	Where different from the issuer, indication of the identity of the person offering to the public or seeking admission to trading of the e-money token	{LEI} or different identifier as specified in Article 14 of [RTS on record keeping]
A.28	Reason for offering to the public or seeking admission to trading of the e-money token by persons referred to in Article 51(1), second	Where the offeror or the person seeking admission to trading is different from the issuer, reason for offering to the public or seeking admission to trading of the e-money token	Free alphanumerical text

	subparagraph, of Regulation (EU) 2023/1114		
<i>Part B - Information about the e-money token</i>			
B.1	Name	Field to be filled in only if a DTI is not provided in field B.14. e-token name	Free alphanumerical text
B.2	Abbreviation	Field to be filled in only if a DTI is not provided in field B.14. e-token abbreviation	Free alphanumerical text
B.3	Details of all natural or legal persons involved in design and development	Details of advisors, development team members, CASPs and all natural and legal persons involved in the design and development of the crypto-asset project, including business addresses or domicile of the company, presented in a tabular format	Free alphanumerical text presented in a tabular format
<i>A description of the characteristics of the e-money token, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109, as specified in accordance with paragraph 8 of that Article</i>			
B.4	Type of white paper	The type of white paper notified.	EMTW
B.5	The type of submission	Type of submission	NEWT = New MODI = Modify

			EROR = Error CORR = Correction
B.6	Crypto-Asset Characteristics	A description of the characteristics of the e-money token.	Free alphanumerical text
B.7	Website of the issuer	Website of the issuer	Free alphanumerical text
B.8	Starting date of offer to the public or admission to trading	Starting date or, if not available at the time of the notification by the competent authority, the intended starting date of offer to the public or admission to trading.	YYYY-MM-DD
B.9	Publication date	Effective or intended publication date of the white paper or of the modified white paper	YYYY-MM-DD
B.10	Any other services provided by the issuer	Any other services provided by the issuer not covered by Regulation (EU) 2023/1114, with a reference to the applicable Union or national law.	Free alphanumerical text
B.11	Identifier of operator of the trading platform	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}
B.12	Language or languages of the white paper	Language or languages in which the crypto-asset white paper is drafted.	Closed list of EU languages

		When multiple languages have been used, this field shall be reported as many times as necessary	
B.13	Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	ISO 24165 Digital Token Identifier
B.14	Functionally Fungible Group Digital Token Identifier, where available	Code used to uniquely identify the functionally fungible group to which the digital asset belongs (i.e., common to each of the several assets to which the white paper relates, i.e. Code used to identify the white paper ISO 24165 DTI of type = 3 (i.e., functionally fungible group), where available	ISO 24165 FFG DTI
B.15	Personal data flag	Flag indicating if the submitted white paper contains personal data	'true' – Yes  'false' – No
B.16	LEI eligibility	Indication that the issuer is eligible for a Legal Entity Identifier .	'true' – eligible  'false' – not eligible

B.17	Home Member State	Home member state as defined in Article 3 paragraph 33 of Regulation (EU) 2023/1114	Closed list of EU member states
B.18	Host Member States	Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114.	Closed list of EU member states
<i>Part C - Information about the offer to the public of the e-money token or its admission to trading</i>			
C.1	Public Offering or Trading	Indication as to whether the crypto-asset white paper concerns an offer to the public of the e-money token or an admission to its trading	'OTPC' – offer to the public 'ATTR' – admission to trading
C.2	Number of units	Where applicable, the total number of units of the e-money token to be offered to the public or admitted to trading	Numerical {DECIMAL-18/3}
C.3	Trading Platforms name	Where applicable, the name of the trading platforms for crypto-assets where admission to trading is sought	Free alphanumerical text
C.4	Trading Platforms Market Identifier Code (MIC)	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}
C.5	Applicable law	The law applicable to the offer to the public of the e-money token	Drop-down list of applicable laws

C.6	Competent court	Competent court	Free alphanumerical text
<i>Part D - Information on the rights and obligations attached to e-money tokens</i>			
D.1	Holder's rights and Obligations	A detailed description of the rights and obligations, if any, that the holder of the e-money token has, including the right of redemption at par value as well as the procedure and conditions for the exercise of those rights	Free alphanumerical text
D.2	Conditions of modifications of rights and obligations	Description of the conditions under which the rights and obligations may be modified	Free alphanumerical text
D.3	Description of the rights of the holders	Description of the rights of the holders when the issuer is not able to fulfil its obligations, including in insolvency	Free alphanumerical text
D.4	Rights in implementation of recovery plan	Description of rights in the context of the implementation of the recovery plan	Free alphanumerical text
D.5	Rights in implementation of redemption plan	Description of the rights in the context of the implementation of the redemption plan	Free alphanumerical text
D.6	Complaint Submission Contact	Contact details for submitting complaints	Free alphanumerical text



D.7	Complaints Handling Procedures	Description of the complaints-handling procedures	Free alphanumerical text
D.8	Dispute Resolution Mechanism	Description of any dispute resolution mechanism or redress procedure established by the issuer of the e-money token	Free alphanumerical text
D.9	Token Value Protection Schemes	Indication as to whether the crypto-asset has a protection scheme protecting the value of the crypto-asset	'true' – Yes  'false' – No
D.10	Token Value Protection Schemes Description	Where the field above is true, a description of protection schemes protecting the value of the crypto-asset and of compensation schemes	Free alphanumerical text
D.11	Compensation Schemes	Indication as to whether the crypto-asset has a compensation schemes	'true' – Yes  'false' – No
D.12	Compensation Schemes Description	Where the field above is true, a description of compensation schemes	Free alphanumerical text Free alphanumerical text
D.13	Applicable law	The law applicable to the e-money token	Drop-down list of applicable laws
D.14	Competent court	Competent court	Free alphanumerical text

<i>Part E - Information on the underlying technology</i>			
E.1	Distributed ledger technology	Field to be filled in only if a DTI is not provided in field B.14. Information on the distributed ledger technology	Free alphanumerical text
E.2	Protocols and technical standards	Information on the protocols and technical standards used, allowing for the holding, storing and transfer of e-money token	Free alphanumerical text
E.3	Technology Used	Other information on the technology used allowing for the holding, storing and transfer of e-money tokens, if relevant	Free alphanumerical text
E.4	Purchaser's technical requirements	Information about the technical requirements that the purchaser has to fulfil to gain control over the e-money token	Free alphanumerical text
E.5	Consensus Mechanism	The consensus mechanism, where applicable	Free alphanumerical text
E.6	Incentive Mechanisms and Applicable Fees	Incentive mechanisms to secure transactions and any fees applicable	Free alphanumerical text
E.7	Use of Distributed Ledger Technology	Indication as to whether the e-money token are issued, transferred and stored using distributed ledger technology that is operated by the issuer or a third-party acting on the issuer's behalf	'true' – Yes, DLT operated by the issuer or a third-party acting on the issuer's behalf

			'false' – No, DLT not operated by the issuer or a third-party acting on the issuer's behalf
E.8	DLT Functionality Description	If the DLT is operated by the issuer or a third party acting on the issuer's behalf, a detailed description of the functioning of such distributed ledger technology	Free alphanumerical text
E.9	Audit	Indication as to whether an audit of the technology used was conducted	'true' – Yes 'false' – No
E.10	Audit outcome	If an audit was conducted, information on the outcome of the audit of the technology used	Free alphanumerical text
G – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts			
G.1	Adverse impacts on climate and other environment-related adverse impacts	Include the information referred to in the Annex to [Delegated Regulation (EU) 2024/XXX on the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts]	Free alphanumerical text

## 8.10 Annex X: Draft RTS pursuant to Article 109(8) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

**supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the data necessary for the classification of crypto-asset white papers and the practical arrangements to ensure that such data is machine-readable**

**(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) No 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<sup>85</sup>, and in particular Article 109(8), third subparagraph, thereof,

Whereas:

- (1) It is important to ensure that investors in crypto-assets are appropriately informed about the characteristics, functions and risks of the crypto-assets they invested in or intend to invest in, and that to that effect the register referred to in Article 109(1) of Regulation (EU) 2023/1114 aims to provide a single portal which investors, crypto-assets holders and other stakeholders can use to search white papers via a standardised set of search criteria. This will contribute to the transparency of the market of crypto-assets and to the accessibility of white papers across the EU.
- (2) In accordance with Regulation (EU) 2023/1114, the classification of a given crypto-asset has a major impact on the applicable requirements. The register should contain information allowing it to facilitate the accessibility of white papers classified on the basis of the categories foreseen by that Regulation and support national competent authorities to verify that the requirements are applied consistently.

---

<sup>85</sup> OJ L 150, 9.6.2023, p. 40.

- (3) To ensure the most efficient operation of the register, national competent authorities should submit the information to ESMA in the same format of the white paper. Furthermore, in order to minimise costs, ESMA and national competent authorities may derive the relevant metadata for the classification of white papers in the Register from the information disclosed in the white papers. In order to minimise the changes in the metadata required as of the date of application of Article 110a of Regulation (EU) 2023/1114, the data used to classify the white papers pursuant to this Regulation should comprise the metadata that national competent authorities will provide to the European Single Access Point (ESAP) in accordance with Article 5 paragraph 1(e) of Regulation (EU) 2023/2859 of the European Parliament and of the Council<sup>86</sup>.
- (4) In order to ensure efficient processing of data, where persons drawing up the white paper are identified in the white papers using an ISO 17442 legal entity identifier (LEI), they should ensure that it is pertinent, valid and duly renewed. Where the issuer does not have a LEI, the register should contain an identifier that ensures similar characteristics and complies with the standard set out in [*Delegated Regulation (EU) xx/xxx on record keeping for crypto-asset service providers*]<sup>87</sup>.
- (5) Since crypto-assets that are not financial instruments cannot at present be described by using the ISO Classification of Financial Instruments (CFI) code, a standard universal method of classification should be developed. In particular, the ISO CFI is being revised to accommodate for the classification of crypto-assets and the revision will not be finalised before the application of this Regulation. Therefore until the revised CFI standard becomes available, an interim classification indicating the type of crypto-assets (crypto-assets other than asset-referenced tokens and e-money tokens, asset-referenced tokens and e-money tokens) should be used. Hence, in order to identify the white papers consistently in the register referred to in Article 109(1) of Regulation (EU) 2023/1114, an international standard identifier for digital tokens, the Functionally Fungible Group Digital Token Identifier (FFG DTI) and the Digital Token Identifiers issued by the Digital Token Identifier Foundation (DTIF) should be used. These identifiers are appropriate as they follow the principles of uniqueness, neutrality, reliability, open source, scalability, accessibility on a cost-recovery basis and they are offered under an appropriate governance framework. Therefore it is appropriate to use the DTI for the purpose of identifying crypto-assets and the FFG DTI to identify white papers pertaining to those crypto assets. Such an identifier allows users to retrieve the main characteristics of the crypto-assets, including their technology-specific features, and to group tokens issued on several blockchains that are pertaining to the same white paper.
- (6) Since this Delegated Regulation concerns the classification of crypto-asset white papers and it is largely linked to the [*Implementing Regulation (EU) xx/xxx on standard forms*,

---

<sup>86</sup> Regulation (EU) 2023/2859 of the European Parliament and of the Council of 13 December 2023 establishing a European single access point providing centralised access to publicly available information of relevance to financial services, capital markets and sustainability (OJ L, 2023/2859, 20.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2859/oj>).

<sup>87</sup> [...]

*formats and templates for the white paper*] it is necessary to align the dates of entry into application of the two. This period of time of deferred application is also necessary to enable persons drawing up white papers and competent authorities to adapt to the requirements laid down in this Delegated Regulation. Its date of application should therefore be deferred to [*the same application date as for the Implementing Regulation (EU) xx/xxx on standard forms, formats and templates for the white paper*]. It is, however, necessary to require that persons drawing up white papers should publish the relevant white papers on their websites in separate sections titled 'White papers' in accordance with the general requirements laid down in Article 6, Article 19 or Article 51 for the period of 1 January 2025 until 31 December 2025.

- (7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (8) ESMA 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<sup>88</sup>,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

#### **Data for the classification of white papers**

1. When submitting a white paper to ESMA register referred to in Article 109(1), point (a), of Regulation (EU) 2023/1114, the competent authority shall provide to ESMA the relevant accompanying data in accordance with the form and standards set out in Tables 1 and 2 in the Annex.
2. The competent authority shall provide the data referred to in paragraph 1 in a common format in accordance with the ISO20022 methodology. Whenever the data referred to in paragraph 1 is provided in the white paper prepared pursuant to Articles 6, 19 or 51 of Regulation (EU) 2023/1114, competent authorities may provide the data referred to in paragraph 1 in the same machine-readable format in which the white paper was prepared

---

<sup>88</sup> 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).

on the basis of [*Implementing Regulation xx/xxx on standard forms, formats and templates for the white paper*].

#### *Article 2*

### **Legal Entity Identifiers**

1. When using the ISO 17442 Legal Entity Identifier, persons drawing up a crypto-asset white paper referred to in Articles 6, 19 or 51 of Regulation (EU) 2023/1114 shall ensure that they are identified with a pertinent, valid and duly renewed code.
2. The persons referred to in paragraph 1 shall ensure that, when ISO 17442 Legal Entity Identifiers are included in the white paper drawn up pursuant to [*Implementing Regulation (EU) xx/xxx on standard forms, formats and templates for the white paper*], the codes are pertinent, valid and issued in accordance to the terms of any of the Local Operating Units of the Global Legal Entity Identifier System and included in the Global Legal Entity Identifier database maintained by the Central Operating Unit appointed by the Regulatory Oversight Committee.

#### *Article 3*

### **Identification of the crypto-asset and the related white paper**

1. When the ISO 24165 Digital Token Identifier is provided, the crypto-assets white paper shall be identified with a valid identifier of type 3 pertaining to the group of crypto-assets to which the white paper relates.
2. When the ISO 24165 Digital Token Identifier is provided, the crypto-asset or crypto-assets to which the white paper relates shall be individually identified with a valid identifier assigned to each of the crypto-assets to which the white paper relates.

#### *Article 4*

### **Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. This Regulation shall apply from [*same application date as the Implementing Regulation (EU) xx/xxx on standard forms, formats and templates for the white paper*].
3. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]



ANNEX

Table 1

**Legend for Table 2**

SYMBOL	DATA TYPE	DEFINITION
{ALPHANUM-n}	Up to n alphanumerical characters	Free text field.
{DATE_TIME_FORMAT}	ISO 8601 date and time format	Date and time in the following format: YYYY-MM-DDThh:mm:ss.dddddZ. – ‘YYYY’ is the year; – ‘MM’ is the month; – ‘DD’ is the day; – ‘T’ – means that the letter ‘T’ shall be used – ‘hh’ is the hour; – ‘mm’ is the minute; – ‘ss.ddddd’ is the second and its fraction of a second; – Z is UTC time. Dates and times shall be recorded in UTC.

{DATEFORMAT}	ISO 8601 date format	Dates shall be formatted in the following format: YYYY-MM-DD.
{DECIMAL-n/m}	Decimal number of up to n digits in total of which up to m digits can be fraction digits	Numerical field for both positive and negative values. – decimal separator is '.' (full stop); – negative numbers are prefixed with '-' (minus); Values are rounded and not truncated.
{DTI}	9 alphanumerical characters	Digital token identifier as defined in ISO 24165 standard
{FFG DTI}	9 alphanumerical characters	Code to identify a group of equivalent Digital token identifiers as defined in ISO 24165 standard type 3
{INTEGER-n}	Integer number of up to n digits in total	Numerical field for both positive and negative integer values.
{LEI}	20 alphanumerical characters	Legal entity identifier as defined in ISO 17442
{MIC}	4 alphanumerical characters	Market identifier as defined in ISO 10383

Table 2

**Data necessary for the classification of white papers in the ESMA register**

Number	Field	Content	Form and standards
1	Type of white paper	<p>The type of white paper notified.</p> <p>Where the white paper concerns asset-referenced tokens, the code 'ARTW' shall be used, where the white paper concerns e-money tokens, the code 'EMTW' shall be used and where the white paper concerns crypto-assets other than asset-referenced tokens and e-money tokens the code 'OTHR' shall be used.</p>	<p>Choice from list of predefined values:</p> <p>'ARTW'</p> <p>'EMTW'</p> <p>'OTHR'</p>
2	Name of the issuer	Name of the issuer	Free alphanumerical text
3	Legal form of the issuer	Legal form	ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)'

4	Legal entity identifier of the issuer, where available	Legal entity identifier of the issuer, where available	{LEI}
5	Other equivalent identifier of the issuer as specified in Article 14 of [RTS on record keeping], where available	Other equivalent identifier of the issuer as specified in Article 14 of [Delegated Regulation (EU) XXXX/XXX on record keeping], where available	Free alphanumerical text
6	Legal entity identifier of the entity that drew up the white paper, where available	Legal entity identifier of the entity that drew up the white paper, where available	{LEI}
7	Other equivalent identifier of the entity that drew up the white paper, where available	Other equivalent identifier of the entity that drew up the white paper as specified in Article 14 of [Delegated Regulation (EU) XXXX/XXX on record keeping], where available	Free alphanumerical text
8	Identifier of operator of the trading platform	Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.	{MIC}
9	Commercial name or trading name	Commercial name or trading name of the issuer, where available	Free alphanumerical text
10	Physical address of the issuer	Physical address of the issuer	Free alphanumerical text

11	Telephone number of the issuer, where available	Telephone number of the issuer, where available	Free alphanumerical text
12	Email of the issuer, where available	Email of the issuer, where available	Free alphanumerical text
13	Website of the issuer	Website of the person drawing up the white paper	Free alphanumerical text
14	Home Member State	Home member state as defined in Article 3 paragraph 33 of Regulation (EU) 2023/1114	Closed list of EU member states
15	Host Member States	Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114.	Closed list of EU member states
16	Starting date of offer to the public or admission to trading	Starting date or, if not available at the time of the notification by the competent authority, the intended starting date of offer to the public or admission to trading.	YYYY-MM-DD
17	Any other services provided by the issuer	Any other services provided by the issuer not covered by Regulation (EU) 2023/1114, with a reference to the applicable Union or national law, where applicable	Free alphanumerical text
18	The date of authorisation	The date of authorisation by the national competent authority, where applicable.	YYYY-MM-DD

19	The date of withdrawal of authorisation	The date of withdrawal of authorisation by the national competent authority, where applicable.	YYYY-MM-DD
20	Publication date	Effective or intended publication date of the white paper or of the modified white paper	YYYY-MM-DD
21	Date and time of notification	Date and time of the latest notification of the white paper to the competent authority	YYYY-MM-DD Thh:mm:ss.dddddZ.
22	Language or languages of the white paper	Language or languages in which the crypto-asset white paper is drafted.  When multiple languages have been used, this field shall be reported as many times as necessary	Closed list of EU languages
23	Record identifier	Unique identifier of the uploaded record, assigned by the sending competent authority	{ALPHANUM-500}
24	Data file reference	Reference code needed to link the data file with corresponding metadata file	{ALPHANUM-500}
25	The type of submission	Type of submission	NEWT = New MODI = Modify EROR = Error CORR = Correction

26	Version	Version of the dataset (data and metadata)	{INTEGER-50}
27	Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available	ISO 24165 Digital Token Identifier
26	Functionally Fungible Group Digital Token Identifier, where available	Code used to uniquely identify the functionally fungible group to which the digital asset belongs (i.e., common to each of the several assets to which the white paper relates, i.e. Code used to identify the white paper ISO 24165 DTI of type = 3 (i.e., functionally fungible group), where available	ISO 24165 FFG DTI
27	Personal data flag	Flag indicating if the submitted white paper contains personal data	'true' – Yes  'false' – No

## 8.11 Annex XI: Draft ITS pursuant to Article 88(4) of MiCA

### COMMISSION IMPLEMENTING REGULATION (EU) .../...

of XXX

**laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to the technical means for appropriate public disclosure of inside information and for delaying the public disclosure of inside information**

**(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 Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>89</sup>, and in particular Article 88(4) third subparagraph thereof,

Whereas:

- (1) Public disclosure of inside information is essential to avoid insider dealing and ensure that investors are not misled. The protection of investors therefore requires timely public disclosure of inside information by issuers, offerors and persons seeking admission to trading.
- (2) Publication of inside information should reach as many investors as possible and be verifiable. The communication of the inside information to the media (dissemination) enables to reach a wide public. The publication of the same information on the websites of issuers, offerors and persons seeking admission to trading allows investors to confirm the reliability of the information disseminated. Therefore, issuers, offerors, and persons seeking admission to trading should comply with both publication on the website and dissemination to ensure effective and reliable disclosure.
- (3) To promote effective distribution of the inside information, issuers, offerors or persons seeking admission to trading should post all inside information that directly concerns them, on their website in the form of a written statement. The document containing the written statement should be downloadable to permit local storage and facilitate further

---

<sup>89</sup> OJ L 150, 9.6.2023, p. 40.



dissemination of the inside information by third parties. The use of the written statement by third parties for publication at their own initiative should not replace the requirement for the issuer, offeror or person seeking admission to trading to communicate the information to the media which are reasonably relied upon by the public.

- (4) To facilitate access to information, the website should allow users to access the information on a non-discriminatory basis and free of charge and to locate the inside information in an easily identifiable dedicated section. Each publication should indicate date and time of the disclosure and publications should be organised in chronological order. Given the cross-border nature of crypto assets trading, it is essential that language barriers do not represent a limit to the access to the published information. In light of this, issuers, offerors and person seeking admission to trading should publish information on their website in the languages in which the crypto-asset white paper is drawn up and, where feasible, a language customary in the sphere of international finance. To facilitate the active distribution of inside information through the website of the issuer, the offeror or the person seeking admission to trading should enable investors to receive push notifications or alerts on any new publication relating to inside information on opt-in basis.
- (5) Given the increasing importance of social media and web-based platforms in conveying information in relation to crypto assets, issuers, offerors and persons seeking admissions to trading may also use social media or web-based platforms to disseminate inside information when they appear to be the media which are reasonably relied upon by the public.
- (6) To ensure that the inside information is disseminated to as wide a public as possible, entities subject to the disclosure obligation should consider disseminating the information through more than one media or type of media whenever a single one is not deemed to be sufficient. When assessing whether a media is reasonably relied upon by the public, entities subject to the disclosure obligation should consider that the use of only one media or type of media with a limited reach should not be considered as reasonably relied upon by the public. This could be, for example, the case of dissemination through a social media platform with a limited number of users.
- (7) To further facilitate access to the publication made directly by the issuer, the offeror or the person seeking admission to trading on their websites, the publication on social media or the web-based platforms should include a link to the page of such websites where the inside information was originally disclosed. Publication on social media and on web-based platforms should occur in line with the general requirements for dissemination, including access to information on a non-discriminatory basis. A non-discriminatory basis for disclosures in social media and web-based platforms should be understood to include only those platforms that are open to the public. While registration requirements from the media are acceptable, invitation-only media would not qualify as non-discriminatory.

- (8) To favour information centralisation, inside information relating to issuers or offerors whose crypto-assets are admitted to trading on a trading platform may be posted for dissemination purposes also on the website of the trading platform, when the trading platform provides this facility. To ensure consistency with the disclosure made by the issuer, the offeror or the person seeking admission to trading, the publication on the trading platforms website should include a link to the page of the website of the issuer, the offeror or the person seeking admission to trading where the information was originally disclosed.
- (9) It is important that the technical means for delaying the disclosure of inside information allow for the maintenance of the key information about the process for delaying the disclosure of inside information, so that issuers, offerors and persons seeking admission to trading are able to fulfil their obligation to notify the competent authorities.
- (10) The notification of the delay of the disclosure of inside information and, where required, the explanation of how all the applicable conditions for the delay were met should be provided to the competent authority in writing using secure electronic means specified by the same competent authority, thereby ensuring the integrity and confidentiality of the content of the information, as well as the rapidity of the transmission.
- (11) To enable the competent authority to identify the relevant persons within the issuer, the offeror or the person seeking admission to trading involved in the delay of disclosure of inside information, the notification of the delay should include the identity of the person who made the notification and of the person or persons responsible for the decision to delay the disclosure of inside information. Likewise, that notification should also indicate the temporal aspects of the delay enabling competent authorities to assess whether the conditions set out in Regulation (EU) 2023/1114 concerning the delay are met.
- (12) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA').
- (13) ESMA has conducted open public consultations on the draft implementing technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Securities Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council<sup>90</sup>,

HAS ADOPTED THIS REGULATION:

---

<sup>90</sup> 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).

## CHAPTER I

### GENERAL PROVISIONS

#### *Article 1*

#### **Definitions**

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

- (a) ‘alert’ means a notification, provided via e-mail, message or pop-up, through which a user is made aware of publications regarding inside information and promotes a swift access to it;
- (b) ‘durable medium’ means any instrument which enables the storage of information in a way that is accessible for future reference for a period of time adequate for the purposes of the information and allows the unchanged reproduction of the information stored;
- (c) ‘electronic means’ are means of electronic equipment for the processing, storage and transmission of data;
- (d) ‘social media’ means an “online social networking service” as defined in point (7) of Article 2 of Regulation (EU) 2022/1925 of the European Parliament and the Council<sup>91</sup>;
- (e) ‘web-based platforms’ means online platforms which collect and disseminate information and data on crypto-assets to promote informed investment decisions, accessible on a non-discriminatory basis and free of charge;
- (f) ‘trading platform for crypto assets’ means one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets.

## CHAPTER II

---

<sup>91</sup> <sup>91</sup> Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).

## **TECHNICAL MEANS FOR APPROPRIATE PUBLIC DISCLOSURE OF INSIDE INFORMATION**

### *Article 2*

#### **Posting of inside information on the website of the issuer, the offeror or the person seeking admission to trading**

1. Issuers, offerors and persons seeking admission to trading for crypto-assets shall post the inside information on their website in the form of a downloadable written statement. The language used in the downloadable written statement to describe the inside information shall be clear, precise and not misleading.
2. The website referred to in paragraph 1 shall comply with all of the following requirements:
  - (a) allow users to access the inside information posted on the website in a non-discriminatory basis and free of charge;
  - (b) allow users to locate the inside information in an easily identifiable section of the website;
  - (c) ensure that the disclosed inside information clearly indicates date and time of disclosure and is organised in chronological order;
  - (d) provide the inside information in the language in which the white-paper of the crypto-asset is drawn up and, where feasible, if the white-paper is not drawn up in a language customary in the sphere of international finance, in a language customary in the sphere of international finance;
  - (e) provide users with the possibility to receive alerts whenever inside information is published.

### *Article 3*

#### **Means for public disclosure of inside information**

1. Issuers, offerors and persons seeking admission to trading for crypto-assets shall disclose inside information using technical means that ensure that inside information is disseminated:
  - (a) to as wide a public as possible on a non-discriminatory basis;

- (b) free of charge; and
  - (c) simultaneously throughout the Union.
2. To ensure effective dissemination, inside information shall be communicated, directly or through a third party, to the media which are reasonably relied upon by the public, including traditional media, social media permitting publication in written form and web-based platforms which permit publication of news related to issuers, offerors or persons seeking admission to trading for crypto-assets. Inside information relating to crypto-assets admitted to trading on a trading platform for crypto-assets may be posted on the website of the trading platform for crypto assets where the crypto-asset is traded, where the trading platform for crypto-assets provides this service.
  3. Issuers, offerors and persons seeking admission to trading shall not disseminate inside information through social media or web-based platforms where the social media or web-based platform does not ensure that the inside information is accessible to all users or where the social media or web-based platform restricts access to users.
  4. Publication on social media, web-based platforms or on the website of the trading platform for crypto-assets for dissemination purposes shall include a link to the written statement published by the issuer, the offeror or the person seeking admission to trading on their websites pursuant to Article 2.
  5. Communications for dissemination of inside information referred to in paragraph 2 shall be transmitted using electronic means that ensure that the completeness, integrity, and confidentiality of the information is maintained during the transmission, and they shall clearly identify:
    - (a) that the information communicated is inside information;
    - (b) the identity of the issuer, the offeror or the person seeking admission to trading (full legal name);
    - (c) the identity of the person making the notification: name, surname, position within the issuer, the offeror or the person seeking admission to trading;
    - (d) the subject matter of the inside information;
    - (e) the date and time of the communication.

Issuers, offerors and persons seeking admission to trading shall ensure the completeness, integrity and confidentiality by remedying any failure or disruption in the communication of inside information without delay.

## TECHNICAL MEANS FOR DELAYING THE PUBLIC DISCLOSURE OF INSIDE INFORMATION

### *Article 4*

#### **Notification of delayed disclosure of inside information and written explanation**

1. For the purpose of delaying the public disclosure of inside information in accordance with Article 88(2) of Regulation (EU) 2023/1114, issuers, offerors and persons seeking admission to trading shall use technical means that ensure the accessibility, readability, and maintenance in a durable medium of all of the following information:
  - (a) the dates and times when:
    - (i) the inside information first existed within the issuer, the offeror or the person seeking admission to trading;
    - (ii) the decision to delay the disclosure of inside information was made;
    - (iii) the issuer, the offeror or the person seeking admission to trading is likely to disclose the inside information;
  - (b) the identity of the persons within the issuer, the offeror or the person seeking admission to trading responsible for:
    - (i) making the decision to delay the disclosure and deciding about the start of the delay and its likely end;
    - (ii) ensuring the on-going monitoring of the conditions for the delay;
    - (iii) deciding about the public disclosure of the inside information;
    - (iv) providing the requested information about the delay and the written explanation to the competent authority;
  - (c) evidence of the initial fulfilment of the conditions referred to in Article 88(2) of Regulation (EU) 2023/1114, and of any change in this fulfilment during the delay period, including:
    - (i) the information barriers which have been put in place internally and with regard to third parties to prevent access to inside information by persons other than those who require it for the normal exercise of their employment,

profession or duties within the issuer, the offeror or the person seeking admission to trading;

(ii) the arrangements put in place in cases where the confidentiality is no longer ensured.

2. Issuers, offerors and persons seeking admission to trading shall transmit to the competent authority a written notification of delay in the disclosure of inside information and a written explanation of such delay through a dedicated contact point within, or designated by, the competent authority, and using the electronic means specified by the competent authority.

Competent authorities shall publish on their website the dedicated contact point within, or designated by, the competent authority and the electronic means referred to in the first subparagraph. Those electronic means shall ensure that completeness, integrity and confidentiality of the information are maintained during the transmission.

3. The electronic means referred to in paragraph 2 shall ensure that the notification of a delay in the disclosure of inside information includes the following information:

(a) the identity of the issuer, the offeror or the person seeking admission to trading: full legal name;

(b) the identity of the person making the notification: name, surname, position within the issuer, the offeror or the person seeking admission to trading;

(c) the contact details of the person making the notification: professional email address and phone number;

(d) identification of the publicly disclosed inside information that was subject to delayed disclosure: title of the disclosure statement; the reference number, where the dissemination system used assigns one; date and time of the public disclosure of the inside information;

(e) date and time of the decision to delay the disclosure of inside information;

(f) the identity of all persons responsible for the decision of delaying the public disclosure of inside information.

4. Where the written explanation of a delay in the disclosure of inside information is provided only upon request of the competent authority in accordance with Article 88(3) of Regulation (EU) 2023/1114, the electronic means referred to in paragraph 2 shall ensure that such written explanation includes the information referred to in paragraph 3.

## CHAPTER IV

### **FINAL PROVISIONS**

#### *Article 6*

#### **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,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]