

# Final Report

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

## Table of Contents

1	Executive Summary .....	2
2	Notification by certain financial entities to provide crypto-asset services .....	3
2.1	Background and legal basis .....	3
2.2	Feedback statement.....	4
3	Information to be included in the application for authorisation as a crypto-asset service provider .....	7
3.1	Background and legal basis .....	7
3.2	Feedback statement.....	8
4	Complaints-handling procedures of crypto-asset service providers .....	11
4.1	Background and legal basis .....	11
4.2	Feedback statement.....	11
5	Assessment of intended acquisition of a qualifying holding in a CASP .....	15
5.1	Background and legal basis .....	15
5.2	Feedback statement.....	16
6	Annexes .....	20
6.1	Annex I – Cost-benefit analysis .....	20
6.2	Annex II – Advice of the Securities and Markets Stakeholder Group .....	41
6.3	Annex III – Draft RTS pursuant to Article 60(13) of MiCA .....	50
6.4	Annex IV – Draft ITS pursuant to Article 60(14) of MiCA .....	65
6.5	Annex V – Draft RTS pursuant to Article 62(5) of MiCA.....	75
6.6	Annex VI – Draft ITS pursuant to Article 62(6) of MiCA .....	100
6.7	Annex VII – Draft RTS pursuant to Article 71(5) of MiCA.....	113
6.8	Annex VIII – Draft RTS pursuant to Article 84 (4) of MiCA.....	126

## 1 Executive Summary

### Reasons for publication

The Regulation on markets in crypto-assets (MiCA)<sup>1</sup> requires ESMA to submit draft regulatory technical standards (RTS) and implementing technical standards (ITS) on a variety of topics.

On 12 July 2023, ESMA published a Consultation Paper to seek stakeholders' views on ESMA's proposals for 5 RTSs and 2 ITSs. The consultation period closed on 20 September 2023. ESMA received 36 responses, 10 of which were confidential. The answers received are available on ESMA's website<sup>2</sup> unless respondents requested otherwise.

ESMA sought the advice of the ESMA Securities and Markets Stakeholder Group's (MSG) established under Regulation (EU) No 1095/2010.

### Contents

Sections 2 to 5 sets out the feedback statements relating to five of the six draft technical standards related to investor protection topics which were included in the aforementioned ESMA public consultation.

The final report relating to the technical standards on conflicts of interest for crypto-asset service providers (in accordance with Article 72(5) of MiCA) will be published at a later stage to allow the European Banking Authority (EBA) to conclude its consultation process and thus allow ESMA and the EBA to cooperate closely and ensure maximum alignment.

Section 6 consists of seven Annexes. Annex I contains the costs/benefit analyses undertaken in relation to the draft technical standards. Annex II contains the advice received by ESMA from the Securities and Markets Stakeholder Group (MSG). Annexes III to VIII contain the draft technical standards.

### Next Steps

The draft technical standards are 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.

---

<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>.

## 2 Notification by certain financial entities to provide crypto-asset services

### 2.1 Background and legal basis

**Article 60(13) of MiCA:**

*ESMA shall, in close cooperation with EBA, develop draft regulatory technical standards to further specify the information 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.*

**Article 60(14) of MiCA:**

*ESMA shall, in close cooperation with EBA, develop draft implementing technical standards to establish standard forms, templates and procedures for the information to be included notification pursuant to paragraph 7.*

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

1. Article 60 of MiCA sets forth the notification requirements for certain financial entities that intend to provide crypto-asset services. Pursuant to Article 60 of MiCA, such entities shall submit the notification to the NCA of their home Member State.
2. Article 60(7) sets forth the information that must be included in the notification. This includes the following main elements:
  - a programme of operations, setting out the types of crypto-asset services that the notifying entity intends to provide, including where and how those services are to be marketed;
  - a description of the notifying entity's internal control mechanisms relating to anti-money laundering and counter-terrorist financing obligations;
  - a description of the notifying entity's procedure for the segregation of clients' crypto-assets and funds;
  - where the notifying entity intends to provide custody and administration of crypto-assets on behalf of clients, a description of the custody and administration policy;
  - documentation of the information and communication technology (ICT) systems and security arrangements of the notifying entity;

- where the notifying entity intends to provide the service of execution of orders for crypto-assets on behalf of clients, a description of the execution policy;
- where the notifying entity intends to provide the service of exchange of crypto-assets for funds or other crypto-assets, a description of the commercial policy.

## 2.2 Feedback statement

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

3. Effectively all respondents expressed support for the draft notification RTS and ITS. While certain respondents stressed the aspect that certain financial entities are already authorized and hence known to NCAs, other respondents emphasized the need for a level playing field in the CASP space and pointed to the fact that crypto-assets are quite different from traditional financial instruments.
4. Some respondents suggested improvements or pointed to deficiencies rooted in the level 1 framework. The fact that not all authorisation requirements are reflected in the notification, finds its origin in level 1. For instance, level 1 does not provide for prudential, governance, information on shareholders or conflicts of interest (other than in the placement context) requirements in the notification. Comments related to such requirements, therefore, could not be taken onboard in this level 2 work. The same is true for complaints handling and identity and proof of good repute of members of the management body.
5. Some respondents requested higher levels of demonstrated crypto-asset expertise with respect to advice and portfolio management services. Others, favoured lower requirements in that regard. ESMA is of the view that CASP advice and portfolio management services are sufficiently different from traditional investment advice and portfolio management to require CASP notifier elaborate on why its personnel is sufficiently qualified to provide such services.
6. With regards to the programme of operations (Article 1 of the draft RTS), some respondents stated that the three-year outlook as required in the draft RTS was excessive and hardly feasible to comply with, particularly due to the high speed of development in the crypto-asset service sector. ESMA, however, is of the view that requiring CASPs to provide a three-year outlook for their business operation prior to entering the crypto-asset services market, is in line with other regulatory frameworks.
7. Other respondents expressed the view that the requirements to describe the impact of the provision of CASP services on other group companies was excessive. ESMA, however, is of the view that where group structures are implemented, such description

can be required, also against the background that complicated group structures and relationships have proven problematic in some recent CASP failures.

8. Furthermore, a few respondents suggested clarifications in the wording related to the requirements for the programme of operations. This included a clarification on what is meant by “categories of clients” or “technical resources”. To facilitate the understanding of the relevant requirements, ESMA included these suggestions.
9. Some respondents requested the inclusion of further notification requirements such as accounting principles to assess the value of crypto-assets, interconnectivity with other CASP providers or traditional financial institutions, effects of a bankruptcy or a hack of the CASP. While potentially pertinent information for national competent authority in the supervisory work, ESMA does not see a basis for the request of such information in the MiCA Level 1 text.
10. One respondent asked for further clarity with regards to the interactions between the business continuity requirements required in Article 3 of the proposed RTS and those in DORA. Article 60(10) of MiCA exempts notifying entities from applying certain MiCA requirements, however the business continuity requirements in Article 68(7) of MiCA are not among those exempted. ESMA is currently preparing an RTS that will further specify business continuity requirements foreseen in Article 68(7) of MiCA. Information to be notified under Article 3 of this RTS should at least relate to requirements in the RTS on business continuity under MiCA. However, business continuity requirements under MiCA as well as under DORA will both apply as relevant.
11. A few respondents commented on Article 5 (Segregation of clients’ crypto-assets and funds) so that the draft RTS would clarify certain operational points linked to the segregation regime under MiCA. As the draft RTS on information to be included in a notification is not the right place to clarify such points, ESMA did not amend Article 5 of the draft RTS.
12. Lastly and in line with Article 70(5) of MiCA, ESMA has clarified that CASPs that are electronic money institutions, payment institutions or credit institutions need not provide in their application file the information required in relation to the segregation of funds. Information relating to the segregation of crypto-assets is, however, still required.
13. A couple of respondents, including the SMSG, pointed to the fact that CASP services are not subject to the Investors Compensation Scheme and suggested that CASPs should lay out to NCAs how they plan on conveying this message to investors. ESMA included such a requirement in the RTS.
14. Regarding Article 7 (*Operating rules of the trading platform and market abuse detection*), one respondent requested the inclusion of a specific description of the expected due diligence to be applied to crypto-assets that are admitted to trading, in particular from an

anti-money laundering perspective. The respondent also suggested deleting the reference to Directive (EU) 2015/849, arguing that this Directive only refers to due diligence applied to customers and not to assets. ESMA does not have the mandate to detail further the due diligence to be carried out by CASPs as part of the approval process before admitting crypto-assets to trading. Article 67(1)(a) of MiCA requires that this customer due diligence must be “commensurate to the money laundering or terrorist financing risk presented by the applicant in accordance with Directive (EU) 2015/849”. This customer due diligence must be aligned with national measures transposing Directive (EU) 2015/849. ESMA has adapted the wording of this requirement to reflect better the intention in Level 1 and has also kept the reference to Directive (EU) 2015/849.

15. Also on Article 7, one respondent suggested that ESMA clarifies the procedure for updating the list of categories of crypto-assets that were flagged as not being admitted to trading in the original notification. ESMA would like to highlight that the ITS on the notification by certain financial entities foresees in its Article 4 that notifying entities have to notify their competent authority of any material changes to the information originally provided in the notification without undue delay. The changes to the information related to categories of crypto-assets that were not admitted to trading in the initial notification should be considered as material change that would require an updated notification, following then the same procedure which was followed for the original one.
16. Finally, concerning Article 7(j), a few respondents suggested that this requirement should foresee not only access by the competent authority to order books but also to any other trading system (ex. liquidity pool). ESMA considers this addition relevant as there might be other trading systems used to collect and execute orders by the trading platform for crypto assets which might not only be order books. Article 7(j) of the RTS has been modified accordingly.

## 3 Information to be included in the application for authorisation as a crypto-asset service provider

### 3.1 Background and legal basis

**Article 62(5) of MiCA:**

*ESMA shall, in close cooperation with EBA, develop draft regulatory technical standards to further specify the information referred to in paragraphs 2 and 3.*

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

**Article 62(6) of MiCA:**

*ESMA shall, in close cooperation with EBA, develop draft implementing technical standards to establish standard forms, templates and procedures for the information to be included in the application for authorisation as a crypto-asset service provider.*

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

17. Article 62 of MiCA provides for the requirements for the application for authorisation as CASP. More particularly, Article 62(1) of MiCA obliges legal persons or other undertakings that intend to provide crypto-asset services to submit their application for an authorisation as a CASP to the NCA of their home Member State.
18. Article 62(2) of MiCA sets out the information that such an application must contain and which encompasses, inter alia, the following elements:
  - information about the identity of the applicant CASP, including the legal name and any other commercial name used by the applicant, the Legal Entity Identifier (LEI) of the applicant and the website operated by the applicant;
  - a programme of operations, setting out the types of crypto-asset services that the applicant CASP intends to provide, including where and how those services are to be marketed;
  - a description of the applicant CASP's governance arrangements and internal control mechanisms (including procedures to comply with anti-money laundering and counter-terrorist financing obligations);
  - a description of the procedure for the segregation of clients' crypto-assets and funds;



- where the applicant CASP intends to provide the service of execution of order for crypto-assets on behalf of clients, a description of the execution policy;
  - where the applicant CASP intends to provide the service of exchange of crypto-assets for funds or other crypto-assets, a description of the commercial policy.
19. Article 62(4) of MiCA sets out that NCAs must not require an applicant CASP to provide any information referred to in Article 62(2) of MiCA that they have already received under the respective authorisation procedures in accordance with Directive 2009/110/EC4, 2014/65/EU5 or (EU) 2015/23666, or pursuant to national law applicable to crypto-asset services prior to the date of entry into force of MiCA, provided that such previously submitted information or documents are still up-to-date.

### 3.2 Feedback statement

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

20. Most respondents, including the SMSG, agreed with the list of information to be provided with an application for authorisation as a CASP, as proposed in ESMA's draft RTS. However, respondents also made proposals on specific elements of the list of information which are addressed below.

#### *Programme of operations*

21. With regards to the programme of operations (Article 2 of the draft RTS), some respondents stated that the three-year outlook as required in the draft RTS was excessive and hardly feasible to comply with, particularly due to the high speed of development in the crypto-asset services sector. ESMA, however, is of the view that such period is in line with other regulatory frameworks, for instance those applicable to investment firms or credit institutions, and that it is reasonable for applicants seeking authorisation as a CASP to provide a programme of operations with a three-year outlook. It seems even desirable that applicants intending to enter the crypto-asset services market have a three-year outlook for their business operations.
22. Finally, a few respondents requested the inclusion of further information requirements in the application for authorisation as a CASP, such as about interconnectivity with other CASP providers or traditional financial institutions, effects of a bankruptcy or a hack of the CASP. While this could be potentially pertinent information for national competent authorities in their supervisory work, ESMA does not see a basis for the request of such information in the application for authorisation as a CASP.

### *Prudential requirements*

23. With respect to Article 3 (*Prudential requirements*) of the draft RTS, a few respondents proposed to further specify the information an applicant must provide on prudential requirements, in particular regarding the undertaking providing the insurance policy. In ESMA's view, this information would have been included in the other type of information already requested in the draft RTS, especially the copy of the insurance policy. However, the draft RTS has been amended to make clear that such information is indeed required.

### *Internal control mechanisms*

24. A respondent raised that the draft RTS should not be requiring, at the authorisation stage, information on how the applicant is managing risks relating to conflicts of interest, in Article 4(2) of the draft RTS, as this is not expressly listed in Article 62 of MiCA. However, ESMA is of the view that the information required under Article 4(2) of the draft RTS is essential for the competent authority assessing the application to ascertain whether the applicant will be able to provide crypto-asset services in accordance with MiCA. In addition, it is clearly part of the information that an applicant must provide as part of its application under Article 62(2)(i) of MiCA. ESMA therefore did not delete the information requirements relating to how the applicant will manage conflicts of interests risks.
25. ESMA would also like to clarify that the information requirements relating to how the applicant will manage conflicts of interest risks relating to remuneration have been maintained. Remuneration policies and practices are an area especially prone to the occurrence of conflicts of interest. It is thus essential that CASPs address these risks and that competent authorities are able to make a first assessment, at the authorisation stage, as to whether the policies and procedures and internal control mechanisms put in place by the applicant are adequate. In addition, MiCA includes a general obligation for CASPs to identify, prevent, manage and disclose conflicts of interests (Article 72 of MiCA). This, of course, includes conflicts of interests that may arise due to the CASP' remuneration policies and practices.

### *Segregation of clients' crypto-assets and funds*

26. A few respondents commented on Article 10 (*Segregation of clients' crypto-assets and funds*) so that the draft RTS would clarify certain operational points linked to the segregation regime under MiCA. As the draft RTS on information to be included in an application for authorisation as a CASP is not the right place to clarify such points, ESMA did not amend Article 10 of the draft RTS.
27. Lastly, and in line with Article 70(5) of MiCA, ESMA clarified that CASPs that are electronic money institutions, payment institutions or credit institutions need not provide

in their application file the information required in relation to the segregation of funds. Information relating to the segregation of crypto-assets is, however, still required.

#### *Operating rules of the trading platform*

28. With regard to Article 12 (Operating rules of the trading platform), the same request to further specify the due diligence to be applied to crypto-assets that are admitted to trading was made by the same respondent. As explained on the section regarding the RTS on notification by certain financial entities, ESMA will not further detail the customer due diligence which should be part of the approval process for admitting crypto-assets to trading.

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

29. Most respondents agreed with ESMA's proposals on standard forms, templates and procedures for the information to be included in the draft ITS on application for authorisation as a CASP. Additionally, some respondents proposed specific amendments to the draft ITS, which are discussed below.
30. A few respondents requested clarification on the requirements related to the notification of changes in Article 4 of the draft ITS. More specifically, such respondents found that notifying "any change" to the initial information provided was not doable. ESMA clarified that only changes that could affect the assessment of the application should be notified.
31. Additionally, ESMA also clarified in Article 4 of the draft ITS that such notification requirements also apply after the authorisation was granted.
32. A few respondents also highlighted the need for the proposed template to allow for smooth and efficient digital processing of the application and communications between the relevant applicant and NCA. However, as the technology and format to be used by NCAs to receive and process applications is not part of ESMA's mandate under Article 62(6) of MiCA, ESMA did not add any provisions in this respect in the draft ITS.
33. Article 109(1)(d) MiCA requires ESMA to establish a register of CASPs which must be publicly available on its website and be updated on a regular basis. Article 109(5) MiCA specifies the information which the register must contain, including the name, legal form and legal entity identifier of the CASP and, where applicable, of the where applicable, of the CASP's branches and the list of crypto-asset services provided by the CASP. To ensure that an application for authorisation also contains all information required for the future ESMA public register of CASPs, ESMA proposes to include a few additional information requirements of limited extent to reflect the requirements of Article 109(5) of MiCA in the draft RTS on the application for authorisation as a CASP.

## 4 Complaints-handling procedures of crypto-asset service providers

### 4.1 Background and legal basis

**Article 71 (5) of MiCA:**

*ESMA, in close cooperation with EBA, shall develop draft regulatory technical standards to further specify the requirements, templates and procedures for handling complaints.*

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

34. Article 71 of MiCA provides for complaints-handling requirements for CASPs. More specifically, Article 71(1) of MiCA requires CASPs to establish and maintain effective and transparent procedures for the prompt, fair and consistent handling of complaints received from clients and to publish descriptions of those procedures.
35. Article 71(2) of MiCA sets out that clients must be able to file complaints free of charge with CASPs.
36. Moreover, Article 71(3) of MiCA requires CASPs to inform clients of the possibility of filing a complaint, to make available to clients a template for filing complaints and to keep a record of all complaints received and any measures taken in response thereto.
37. Article 71(4) of MiCA stipulates that CASPs are obliged to investigate all complaints in a timely and fair manner and to communicate the outcome of such investigations to their clients within a reasonable period of time.
38. Article 71(5) of MiCA requires ESMA, in close cooperation with EBA, to develop draft RTS to further specify the requirements, templates and procedures for handling complaints and to submit these draft RTSs to the Commission by 12 months after the date of entry into force of MiCA.

### 4.2 Feedback statement

39. The feedback received was mostly positive with, however, some specific and more technical points raised by respondents relating to language requirements, analysis of complaints-handling data or use of the template.

40. One more general point was raised by a few respondents regarding the alignment of ESMA's draft RTS on complaints handling by CASPs and EBA's draft RTS on complaints-handling by issuers of asset-referenced tokens.
41. ESMA's response to each of these points can be found below.

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

42. Most respondents agreed with ESMA's proposals on the requirements, templates and procedures for CASPs' handling of client complaints. Some respondents, however, suggested specific amendments to ESMA's proposed draft RTS, which are addressed below.
43. Some respondents expressed concerns relating to the language requirements for the publication of CASPs' description of the complaints handling procedure and clients' filing of complaints. These respondents consider ESMA's proposals as too burdensome, especially for CASPs which plan to provide their service through passporting in several EU Member States.
44. After further consideration, ESMA decided to amend the language requirements applicable to CASPs under the draft RTS and to, instead, require, CASPs to publish the description of the complaints handling procedure and the standard template in all languages used by the CASP to market its services or communicate with clients. However, CASPs should still accept complaints filed in any of the aforementioned languages as well as in the official languages of the home Member State and host Member States that are also official languages of the Union. This is to ensure that a broad range of clients can express their problems and dissatisfaction with the services they receive.
45. Secondly, some respondents were concerned that the template in the draft RTS was meant as a rigid method of filing complaints for clients (requiring a pdf file to be sent by email for instance). ESMA would like to clarify that the inclusion of the template in the draft RTS should by no means be read as requiring its mandatory use by clients to file an admissible complaint with their CASP. In addition, CASPs may adapt how clients may fill in the template to submit their complaints. It could be through digitalisation of the template, including drop-down menus or other formats that CASPs may deem more user-friendly, for instance. However, CASPs shall not deem a complaint inadmissible on the sole ground that a client used the template to file his or her complaint instead of any other methods that the CASP may make available to them, as an alternative.
46. Furthermore, some respondents were of the view that requiring ongoing analysis of complaints-handling data by CASPs to ensure consistent complaints-handling was

disproportionate. After further consideration, Article 8 of the draft RTS was not amended as it was deemed important that CASPs be able to be aware at all times of complaints received and any issues in their handling.

47. Few respondents also raised that requiring a separate complaints-handling function was disproportionate. ESMA would like to clarify that this is not a requirement under Article 2 of the draft RTS. CASPs shall dedicate adequate resources to the management of complaints. Depending on, among other criteria, the size and range of services of the CASP, such resources may not be solely dedicated to the management of complaints. However, such resources should be adequate for the proper handling of complaints.
48. Lastly, few respondents (including the SMSG) expressed the view that the requirements relating to complaints handling applicable to CASPs and issuers of asset-referenced tokens should be further aligned. In their view, complaints-handling rules should be uniform for CASPs and issuers of asset-referenced tokens, as some firms may engage as both under MiCA. Most of the respondents who expressed such view, however, did not specify which approach should be followed between ESMA's more detailed requirements and the EBA's principle-based approach.
49. As previously stated in the consultation paper<sup>3</sup>, in ESMA's view, the crypto-asset services market is still at an early stage of development and it is essential to enable clients to express their problems and dissatisfaction with the services they receive, in a uniform way across the Union, to promote investor protection and a shared culture of complaints-handling by CASPs. As CASPs have so far and for the most part been unregulated, the compliance gap between the current situation and where CASPs should get at is important.
50. In addition, the difference of approach may also be explained by the different business models of issuers of asset-referenced tokens and CASPs. Indeed, the variety of interactions and situations resulting from the activities of CASPs is, in ESMA's view, more prone to situations where a client would have a complaint against a CASP, compared to holders of asset-referenced tokens and their interactions with issuers of asset-referenced tokens (interactions which should be more sporadic, therefore would not give rise to so many complaints and for which high level rules on complaints handling may be appropriate).
51. For the above reasons, ESMA remains of the view that the complaints-handling requirements applicable to CASPs under MiCA should be rather specific (instead of high-level and principle-based). In addition, ESMA notes that the two sets of requirements applicable to complaints handling by CASPs, on one hand, and issuers of asset-

---

<sup>3</sup> [ESMA74-449133380-425](#).

referenced tokens, on the other hand, as presented in the consultation paper, were not inconsistent.

52. That being said, the EBA and ESMA have worked in close cooperation in finalising the respective Final Reports to further align the two draft RTSs and have reached common positions on a number of important points, including the language requirements, full alignment for the templates, the obligation for CASPs and issuers of asset-referenced tokens to provide a copy of the complaint where it is submitted through an online form, etc.

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

53. Most respondents that expressed their view were against keeping this requirement in the draft RTS. These respondents were of the view that the handling of paper-based complaints (e.g. check for admissibility of complaint) and their record keeping would be more complex and could hamper the efficiency of the complaints-handling procedure. However, a few respondents were in favour of keeping the option for CASPs' clients to submit their complaints by post. These respondents stated that some retail clients might only use paper-based communication.
54. After further consideration and to mitigate the risk of excluding certain groups of clients from an effective communication related to complaints with CASPs, ESMA has decided to keep the obligation for CASPs to also admit complaints submitted in paper form in the draft RTS.



## 5 Assessment of intended acquisition of a qualifying holding in a CASP

### 5.1 Background and legal basis

#### Article 84 (4) of MiCA:

ESMA, in close cooperation with EBA, shall develop draft regulatory technical standards specifying the detailed content of the information that is necessary to carry out the assessment referred to in Article 83(4), first subparagraph. The information required shall be relevant for a prudential assessment, proportionate and adapted to the nature of the proposed acquirer and the proposed acquisition referred to in Article 83(1).

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

55. Article 83 of MiCA requires any natural or legal person who intends to acquire or to increase a qualifying holding in a CASP, to notify the NCA of that CASP in writing and provide specific information to enable the relevant NCA to assess the proposed acquisition or increase of an existing qualifying holding.
56. Article 84 of MiCA further establishes the criteria against which the NCA should evaluate the suitability of the proposed acquirer. These criteria include the following: a) reputation of the proposed acquirer; b) reputation and experience of any person that will direct the business of the CASP as a result of the intended acquisition; c) financial soundness of the proposed acquirer; d) continued compliance of target CASP with applicable MiCA requirements after the acquisition; e) reasonable grounds to suspect money laundering or terrorist financing in connection with the proposed acquisition or whether it could increase these risks.
57. ESMA is mandated in Article 84(4) of MiCA to develop, in close cooperation with EBA, draft regulatory technical standards (RTS) on the detailed content of the information for the assessment of proposed acquisitions of qualifying holdings in CASPs. The aim of this draft RTS is to specify the detailed content of the information that direct or indirect proposed acquirers must provide to national competent authorities (NCAs) when notifying the intended acquisition. This should ensure a harmonised approach to the assessment across Member States in the EU of the intended acquisition of qualifying holdings in CASPs.
58. The RTSs are applicable to proposed acquirers of qualifying holdings in CASPs, as well as NCAs as designated under Article 93(1) of MiCA that will conduct the assessment of the intended acquisition in accordance with Article 83(4) of MiCA.



## 5.2 Feedback statement

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

59. Respondents' views with regard to this question were mixed. Some respondents argued that some of the requirements in the proposed RTS would be stricter than requirements applicable to entities willing to acquire a qualifying holding in a firm regulated under MiFID. Other respondents agreed with ESMA's proposal. ESMA would like to highlight that in order to produce these RTS, the requirements applicable to entities proposing to acquire a qualifying holding in an investment firm have been considered and adapted in the draft RTS under MiCA taking into consideration the specificities of the business of crypto-assets services providers.
60. One respondent questioned the relevance of some of the information about the intended acquisition. In particular, this respondent suggested that the content of any intended shareholder's agreement with other shareholders in relation to the target entity may be overly intrusive for the parties to the transaction as it may reveal sensitive and confidential business information which might not be needed for the assessment made by the competent authority. ESMA notes that this information is required for the assessment of any proposed acquisition of a qualifying holding and it is necessary to allow the competent authority to have a complete view of the proposed acquisition.
61. One respondent suggested that a transitional period should be granted for proposed acquirers that have been operating for longer than three years but are not required to provide audited accounts by its third-country supervisor. ESMA has clarified the drafting to make clear that only when financial statements are audited externally, should the proposed acquirer provide them audited. This is in line with existing requirements applicable to proposed acquisitions of qualifying holdings in investment firms.
62. One respondent questioned the need for the description of the performance of a qualifying holding previously acquired by AIFs or UCITs, arguing that the suitability of the proposed acquirer cannot be inferred from the analysis of this information which does not entirely depend on the skills and experience of the proposed acquirer. This respondent also suggested clarifying that declarations of honour do not need to be resubmitted if the assessment by the NCA lasts for more than three months, questioned the need for the information on any dismissal from a previous employment or removal from a fiduciary relationship and asked to clarify whether the comprehensive assessment of the structure of the shareholding of the target entity is to be done by the competent authority or the proposed acquirer. ESMA would like to recall that the description of the performance of qualifying holdings previously acquired by AIFs or UCITs is an essential element of the assessment of professional competence by the competent authority. With

regards to the declaration of honours, and all other information submitted by the proposed acquirer, ESMA has added a recital to clarify that this information has to be true, accurate, complete and up-to-date from the moment of submission of the notification until the completion of the assessment by the competent authority. Therefore, proposed acquirers should inform competent authorities in the event of a change to the information provided during the period of assessment. Finally, with regard to the assessment of the structure of the shareholding, ESMA has amended the wording to ensure alignment with the RTS on the information required for the assessment of proposed acquisitions of qualifying holdings on issuers of ARTs, prepared by EBA. This wording clarifies that the proposed acquirer is responsible for the due diligence which will allow them to understand the influence exercised by the qualifying holding and whether Articles 9 or 10 would apply in each case.

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

63. All respondents agreed with ESMA's proposed approach. Only one respondent added that information on the "overall IT and technology architecture" of the proposed acquirer should be also provided by proposed acquirers of qualifying holdings of less than 50%. ESMA notes that this information does not seem relevant and proportionate for proposed acquirers of qualifying holdings of less than 50%. It would also represent a significant departure from the existing framework applicable to proposed acquisitions of qualifying holdings on investment firms.

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

64. Most of the respondents who considered this question relevant to them indicated in clear terms support for the list of information required to assess the financing of the acquisition, with a few of them not making any further comments.
65. One respondent noted that some requirements may be inapplicable to certain acquisitions, for instance where the acquisition is not financed with crypto-assets, while another questioned the necessity of – and the burden imposed by – the following proposed requirements:
- "any assets, including any crypto-assets, which are to be sold to help finance the proposed acquisition (...)",
  - "details on access to capital sources and financial markets including details of financial instruments to be issued";

- “the wallet where the crypto-assets used or exchanged into official currency to acquire the holding were stored, of the crypto-asset service providers used and of the address identifiers of the originator and of the beneficiary on the DLT”, and
  - “information on any financial arrangement with other persons who are or will be shareholders of the crypto-asset service provider”.
66. At the same time, one respondent suggested requesting further details on the wallets, protocols and networks used.
67. One respondent asked that e-money tokens (EMTs) be excluded from the scope of application of requirements specific to assets used for the funding of acquisitions given their legal status as electronic money.
68. Finally, one respondent mentioned the variety of possible deal structures, including earn out arrangements.
69. ESMA notes the support for the proposed list and notes that requirements which are not relevant to all acquisitions should remain but be marked as N/A by the proposed acquirer, where appropriate. ESMA acknowledges the considerations relating to the burden imposed by certain proposed requirements but notes that these requirements appear standard across existing financial legislation, and notes that introducing the notion of “significant financial arrangements” would introduce subjectivity. Further, ESMA notes that regarding earn-out arrangements, as part of the assessment of the proposed acquirer’s financial soundness and of the financing of the transaction, the competent authority has to check all sources of financing of the purchase price at the time of the assessment of the proposed acquisition. ESMA acknowledges the status of EMTs as electronic money while noting that this does not require specification in the RTS. Finally, ESMA agrees to add further details with regards to wallets, protocols and networks used, while noting that asset management contracts should already be covered in the section related to proposed acquirers that are funds.

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

70. All answers to this question agreed with the identified cases where reduced information requirements apply, and with the related requirements and safeguards.
71. One respondent indicated that in their view Article 12 on the reduced information requirements should apply to proposed acquirers having been assessed for the acquisition or increase in qualifying holdings by any EU NCA within the two previous years, rather than just to proposed acquirers having been assessed in the previous two years for the acquisition or increase in qualified holdings by the same competent authority as that of their current target entity.

72. While ESMA agrees with the idea in principle, on balance it appears complex to extend the scope of reduced information requirements in the proposed way as this would imply the NCA responsible for the assessment of the new acquisition retaining legal responsibility for the approval of the elements that were in reality approved by the NCA responsible for the assessment of the previous acquisition, on the basis of documents that were not provided to the NCA responsible for the new acquisition.

## 6 Annexes

### 6.1 Annex I – Cost-benefit analysis

#### 6.1.1 RTS and ITS on the information to be included in the application for authorisation as crypto-asset service provider

*Impact of the draft RTS and ITS under Article 62(5) and (6) of MiCA*

1. 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.
2. MiCA sets out a new legal framework applicable to legal persons or other undertakings intending to provide crypto-asset services, requiring such entities to submit an application for authorisation containing all the information set out in Article 62(2) of MiCA, as specified by the RTS on the information for authorisation as a CASP.
3. The next paragraphs present the cost-benefit analysis of the main policy options included in this final report on the requirements for the application for authorisation as a CASP under Article 62 of MiCA.

*Problem identification*

4. The application for authorisation submitted to the competent authority must include all the information set out in the RTS on information for authorisation, with the appropriate level of detail to enable the competent authority to carry out the assessment of the application and to inform its decision to grant or not the authorisation.
5. Lack of a standardised information in the application for authorisation may lead to diverging approaches and different practices across Member States with respect to the granting of authorisations, hindering the level playing field and leading to regulatory arbitrage across EU Member States. Against this background, MiCA mandates ESMA, in close cooperation with the EBA, to develop i) an RTS to specify the information to be contained in the application for authorisation to provide crypto-asset services and ii) and ITS to establish standard forms, templates and procedures for the application.
6. In addition, by screening the market participants authorised to provide crypto-asset services, competent authorities provide a safer space for investors, despite the risks that any investment in crypto-assets represents.

### *Policy objectives*

7. The strategic objective of the draft RTS and ITS is to harmonise the requirements related to the content and submission of applications for the authorisation as CASPs. More specifically, the draft RTS aims at specifying the detailed list of information to be provided to the competent authorities in the application for the authorisation as CASPs. The draft ITS aims at ensuring consistency in the application process by setting out specific templates for the information to be included in the application and by clarifying the procedure.

### *Baseline scenario*

8. The baseline scenario is the situation where applicants for authorisation as a CASP must comply with their obligations under Article 62 of MiCA, without any further specification of these requirements by any draft RTS and ITS. Thus, competent authorities would request information from applicants to inform their assessments as part of the process for granting and refusing requests for authorisation as CASPs, based on the requirements set out in Article 62(2) and (3) of MiCA.
9. As these information requirements have a rather general nature, this may have a twofold significant impact. Firstly, the information contained in the applications may be rather high-level and lack appropriate detail. This may not enable competent authorities to swiftly and effectively assess whether the applicant is capable and ready to comply with the relevant requirements of the MiCA framework. Ultimately, this carries the risk that inter alia applicants' internal arrangements and procedures related to governance and internal control mechanisms or segregation of clients' crypto-assets and funds may turn out to be less robust than presented to competent authorities in the high-level content of the application
10. Secondly, the information requested by competent authorities may diverge significantly across Member States. This may result in competent authorities taking diverging approaches to grant authorisation to applicants. Finally, this can lead to regulatory arbitrage between Member States, with applicants opting for jurisdictions where competent authorities grant authorisation through a more permissive approach.

### *Options considered and preferred options*

11. This section presents the main policy options discussed and the decisions made when developing the draft RTS and draft ITS. The policy options' respective advantages and disadvantages and the preferred options resulting from this analysis are assessed below.

## Policy issue 1: Level of detail of the required information to assess the application for authorisation as a CASP

12. ESMA considered two policy options:
  - Option 1a: Set out high-level requirements in the draft RTS and draft ITS for the information to be included in the application for authorisation as a CASP
  - Option 1b: Specify the requirements in the draft RTS and draft ITS for the information to be included in the application for authorisation as a CASP with a level of detail enabling the competent authority to carry out a meaningful assessment.
13. An important initial step of a competent authority's authorisation process is to check whether the application is complete. On this basis, the competent authority assesses the submitted information on whether the applicant is capable and ready to comply with the relevant requirements of the MiCA framework. However, if the requirements for the information to be included in the application are set out in the draft RTS and draft ITS as high-level provisions without appropriate specification (Option 1a), the competent authority may have to request additional information from applicants to be able to conduct a meaningful assessment on whether authorisation should be granted or not. This may cause inefficiencies in assessments and potential rejections due to the lack of sufficiently substantiated information in the applications.
14. To allow a competent authority to assess meaningfully an application, this application should not only include information on the relevant obligations of the MiCA framework. Instead, in particular, this application must contain all the required information in appropriate detail to enable the competent authority to effectively assess whether the applicant complies with the relevant MiCA requirements and should be granted authorisation, or not.
15. Thus, Option 1b was chosen as the preferred option.

### *Cost-benefit analysis*

16. The draft RTS and draft ITS on information for authorisation as a CASP are expected to result in both costs and benefits to applicants and competent authorities.

### *Costs*

17. Applicants will mostly incur one-off costs related to the collection of data and the preparation of the application for authorisation. They will also incur ongoing costs for the monitoring and notification to the competent authority of any material change.



18. For competent authorities, the costs relate to the resources required for the assessment of the application. In Member States where a pre-MiCA national framework on the provision of crypto-assets services exists, competent authorities may incur one-off costs as they may have to amend their internal application process to be able request from applicants the specific required information proposed by the draft RTS and to ensure that applicants can submit this information via the draft ITS's standard forms, templates and procedures. In jurisdictions where no pre-MiCA national framework on the provision of crypto-assets services exists, competent authorities will have to set up an internal procedure for the processing and assessment of application.
19. It should be preliminary observed that since the requirements on the information for application for authorisation as CASP are provided under MiCA, the impact of the draft RTS and ITS should be considered having in mind those legal provisions that they specify.

#### *Benefits*

20. In terms of benefits, the draft RTS and ITS will promote convergence and foster clarity and predictability for applicants on the authorisation process. The harmonised application requirements also promote fair competition between CASPs at the authorisation stage, no matter their home Member State.

*Table: Costs and benefits of the draft RTS and ITS on the required information for authorisation as a CASP*

<b>Stakeholder groups affected</b>	<b>Costs</b>	<b>Benefits</b>
<b>Applicant CASPs</b>	<p>Initial one-off costs to gather the required data and prepare the application.</p> <p>Ongoing costs to monitor material changes and notify them to the relevant competent authority.</p>	<p>Clarity and predictability of the information required for an application.</p> <p>Level-playing field at the entry point.</p>
<b>Competent authorities</b>	<p>Initial one-off costs to amend or implement internal process for authorisation.</p> <p>Ongoing costs to assess the applications.</p>	<p>Harmonisation and level-playing field.</p> <p>Clarity on the necessary level of detail required in applications.</p>



## **6.1.2 RTS and ITS on the notification by certain financial entities to provide crypto-asset services**

### *Impact of the draft RTS and ITS under Article 60(13) and (14) of MiCA*

21. 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.
22. MiCA sets out a new legal framework applicable to certain financial entities intending to provide crypto-asset services, requiring such entities to notify all the information set out in Article 60(7) of MiCA, as specified by the RTS on the notification by certain financial entities to provide crypto-asset services.
23. The next paragraphs present the cost-benefit analysis of the main policy options included in this final report on the requirements for the notification by certain financial entities to provide crypto-asset services under Article 60 of MiCA.

### *Problem identification*

24. The notification submitted by certain financial entities to their competent authority to provide crypto-asset services must include all the information set out in the draft RTS, with the appropriate level of detail to enable the competent authority to then supervise the provision of crypto-asset services by such financial entities.
25. Lack of standardised information requirements at the notification stage may lead to diverging approaches and different practices across Member States, hindering the level-playing field between CASPs. Against this background, MiCA mandates ESMA, in close cooperation with the EBA, to develop i) an RTS to specify the information to be contained in the notification to provide crypto-asset services and ii) and ITS to establish standard forms, templates and procedures for the notification.

### *Policy objectives*

26. The strategic objective of the draft RTS and ITS is to harmonise the requirements related to the content and submission of notifications to provide crypto-asset services by certain financial entities. More specifically, the draft RTS aims at specifying the detailed list of information to be provided to the competent authorities in the notification. The draft ITS aims at ensuring consistency in the notification process by setting out specific templates for the information to be included and by clarifying the procedure.

### *Baseline scenario*

27. The baseline scenario is the situation where financial entities notifying their intentions to provide crypto-asset services must comply with their obligations under Article 60 of MiCA, without any further specification of these requirements by any draft RTS and ITS.
28. As these information requirements have a rather general nature, this may have a twofold significant impact. Firstly, the information contained in the notifications may be rather high-level and lack appropriate detail. This may not enable competent authorities to get the adequate information for their then ongoing supervision of the crypto-asset services of such financial entities.
29. Secondly, the information requested by competent authorities may diverge significantly across Member States and create an uneven level-playing field.

### *Options considered and preferred options*

30. This section presents the main policy options discussed and the decisions made when developing the draft RTS and draft ITS. The policy options' respective advantages and disadvantages and the preferred options resulting from this analysis are assessed below.

### **Policy issue 1: Level of detail of the required information to be included in the notification to provide crypto-asset services**

31. ESMA considered two policy options:
  - Option 1a: Set out high-level requirements in the draft RTS and draft ITS for the information to be included in the notification to provide crypto-asset services
  - Option 1b: Specify the requirements in the draft RTS and draft ITS for the information to be included in the notification to provide crypto-asset services with a level of detail enabling the competent authority to then carry out a meaningful ongoing supervision.
32. If the requirements for the information to be included in the notification are set out in the draft RTS and draft ITS as high-level provisions without appropriate specification (Option 1a), the competent authority may soon have to request additional information to be able to conduct a meaningful supervision of the financial entity providing crypto-asset services.
33. In addition, this may create an uneven level-playing field between financial entities submitting a notification to provide crypto-asset services and applicants for authorisation as crypto-asset service providers under Article 62 of MiCA. The different treatment (notification versus authorisation) and the different list of information to be provided is justified on the basis of the status of the financial entities and the fact that they are already known to and supervised by their competent authority (therefore, there is no need to resubmit information already provided previously). However, for the information

that must be provided by both types of entities under Articles 60 and 62 of MiCA, a different treatment would not be justified.

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

#### *Cost-benefit analysis*

35. The draft RTS and draft ITS on notification by certain financial entities to provide crypto-asset services are expected to result in both costs and benefits to financial entities submitting a notification and competent authorities.

#### *Costs*

36. Financial entities notifying their intention to provide crypto-asset services will mostly incur one-off costs related to the collection of data and the preparation of the notification. They will also incur ongoing costs for the monitoring and notification to the competent authority of any material change.

37. For competent authorities, the costs relate to the resources required to analyse the information provided. In Member States where a pre-MiCA national framework on the provision of crypto-assets services exists, competent authorities may incur one-off costs as they may have to amend their internal processes to be able to request from financial entities notifying their intention to provide crypto-asset services the specific required information proposed by the draft RTS and to ensure that such entities can submit this information via the draft ITS's standard forms, templates and procedures. In jurisdictions where no pre-MiCA national framework on the provision of crypto-assets services exists, competent authorities will have to set up an internal procedure for the processing and analysis of the information submitted.

38. It should be preliminary observed that since the requirements on the information for the notification by certain financial entities to provide crypto-asset services are provided under MiCA, the impact of the draft RTS and ITS should be considered having in mind those legal provisions that they specify.

#### *Benefits*

39. In terms of benefits, the draft RTS and ITS will promote convergence and foster clarity and predictability for financial entities intending to provide crypto-asset services on the notification process. The harmonised notification requirements also promote fair competition between financial entities at the notification stage, no matter their home Member State. This also prevents creating, at level 2, an uneven level-playing field between applicant CASPs and such financial entities.

*Table: Costs and benefits of the draft RTS and ITS on the required information for notification by certain financial entities to provide crypto-asset services*

Stakeholder groups affected	Costs	Benefits
<b>Financial entities notifying their intention to provide crypto-asset services</b>	<p>Initial one-off costs to gather the required data and prepare the notification.</p> <p>Ongoing costs to monitor material changes and notify them to the relevant competent authority.</p>	<p>Clarity and predictability of the information required for a notification.</p> <p>Level-playing field at the entry point.</p>
<b>Competent authorities</b>	<p>Initial one-off costs to amend or implement internal process for notifications.</p> <p>Ongoing costs to assess the information provided.</p>	<p>Harmonisation and level-playing field.</p> <p>Clarity on the necessary level of detail required in notifications.</p>

### 6.1.3 RTS in relation to complaints-handling by CASPs

#### *Impact of the draft RTS under Article 71(5) of MiCA*

40. As per Article 10(1) of Regulation (EU) No 1095/2010, any draft regulatory technical standards developed by ESMA shall be accompanied by an analysis of ‘the potential related costs and benefits’ of the technical standard.
41. The next paragraphs present the cost-benefit analysis of the main policy options included in this final report on the requirements for complaints-handling by CASPs under Article 71 of MiCA.

#### *Problem identification*

42. Article 71 of MiCA imposes complaints-handling requirements on CASPs. These relate to complaint handling procedures, client information about complaints-handling, the template made available to clients to file a complaint, record-keeping of complaints and complaints-handling measures as well as CASPs’ investigations of and responses to complaints. Article 71(5) requires ESMA to develop a draft RTS to specify the requirements, templates and procedures for handling complaints.
43. However, Article 71 of MiCA does not specify what the complaints-handling procedures of CASPs should include, nor how CASPs should communicate with clients about their complaints-handling process or provides the template for the submission of a complaint. This could lead to a lack of harmonisation in CASPs’ practices regarding complaints-handling. This situation could also undermine the objective of Article 71 of MiCA which is to protect investors by ensuring that clients of CASPs are informed about the possibility to file a complaint, how to submit their complaint and that CASPs handle complaints received from clients in a prompt, fair and consistent manner.

#### *Policy objectives*

44. The general objective of the draft RTS is to specify the requirements applicable for handling complaints, provide a template that clients of CASPs may use to file a complaint with any CASP in the Union and give more information on what the procedures for handling complaints should include.
45. More specifically, the draft RTS aim to ensure consistency of the requirements applicable to and the procedures for complaints handling by CASPs, and consistency of the information provided by CASPs, with a view to ensure harmonised application and supervision of Article 71 of MiCA across the Union.

### *Baseline scenario*

46. The baseline scenario is the situation where CASPs have to comply with their obligations under Article 71 of MiCA, without any further specification. However, Article 71(5) of MiCA gives ESMA a mandate to specify the requirements, templates and procedures for handling complaints, thereby indicating that further details where desirable to ensure that the objectives of Article 71 of MiCA were attained.
47. Indeed, in a market at still an early stage of development, such as the crypto-asset service market, it is necessary to ensure a certain level of detail with regards to the requirements, templates and procedures for handling complaints, as some CASPs may not be familiar with the level of care expected from a regulated entity when handling complaints from clients.
48. With the entry into force of MiCA, CASPs must comply with Article 71 of MiCA. The legal requirements provided by Article 71 thus form the baseline scenario of the IA, i.e. the impact caused by MiCA is not assessed within this IA, which focuses only on areas where further specifications have been provided in the draft RTS.
49. ESMA's objective in drafting the RTS is to promote investor protection and a shared culture of complaints handling by CASPs by ensuring that clients are enabled to express in a uniform way across the Union their dissatisfaction with crypto-asset services provided by CASPs.

### *Options considered and preferred options*

#### **Policy issue 1: CASPs procedures for handling complaints**

50. The first element of the legal mandate for the RTS on complaints-handling by CASPs under Article 71 of MiCA requires ESMA to specify the procedures for the prompt, fair and consistent handling of complaints received from clients by CASPs. In this context, ESMA considered three policy options:
  - Option 1a. Provide for a general obligation for CASPs to draft complaints-handling procedures, without further specification as to their content;
  - Option 1b. Provide the list of information/topics that CASPs' procedures for handling complaints should contain;
  - Option 1c. Provide a baseline template or even a rigid template for CASPs' procedures for handling complaints.
51. Option 1a was regarded as not properly fulfilling the mandate as it would only replicate level 1 requirements (while the mandate requires ESMA to "specify [...] the procedures

*for handling complaints*". It would also not ensure an appropriate level of harmonisation across the EU nor ensure that CASPs have sufficiently detailed procedures for the prompt, fair and consistent handling of complaints.

52. Option 1b would ensure a minimum level of harmonisation by ensuring that CASPs' complaints-handling procedures are sufficiently standardised and comparable in the EU and that they deal with certain topics deemed as essential for the prompt, fair and consistent handling of complaints received by clients. Option 1b is however sufficiently high level to allow CASPs to adapt their procedures to the scale, nature and range of crypto-asset services provided as well as their organisation, number of complaints received, etc.
53. Option 1c, on the other hand, was regarded as too prescriptive and not necessary to achieve the desired level of investor protection.
54. Therefore, Option 1b has been chosen as the preferred option.

## Policy issue 2: Language requirements

55. Article 71 of MiCA provides for a number of measures to ensure that clients are aware of the possibility to file a complaint free of charge with their CASPs and how to do so (CASPs are thus required to publish a description of their complaints-handling procedures). In this context, ESMA considered two policy options:
  - Option 2a. Remain silent on the language requirements;
  - Option 2b. Provide for some minimum language requirements that CASPs have to comply with to ensure that clients are duly informed (i.e. in a language that they understand) about the possibility and how to submit a complaint as well as the languages in which a complaint may be filed.
56. As crypto-asset services are, for the vast majority, provided online and as MiCA puts no barriers to the provision of cross-border services across the Union, it is very easy for crypto-asset service providers to reach clients across the EU. Therefore, CASPs may be established and operate from any EU jurisdictions but may easily reach consumers everywhere in the Union.
57. Under Option 2a, CASPs would have no obligation to make the information about their complaints-handling procedures available in any specific language. This may lead to a CASP established, for instance, in France or in Lithuania, to only publish such information in French or in Lithuanian, respectively, even though such CASP may have clients in Spain, Germany, The Netherlands, etc. The information requirements provided under Article 71 may thus become ineffective, if information is provided in a language



not understood by the client. Article 71 may also not reach its goal if CASPs put language barriers to clients filing a complaint.

58. To ensure that the information obligations under Article 71 reach their objective (i.e. effectively inform clients about the possibility of and how to submit a complaint with their CASPs), Option 2b compels CASPs to inform client about the possibility to submit a complaint free of charge and to publish the description of their complaints-handling procedures in a number of languages which correspond to those used by the CASP to market its services or communicate with clients. Where CASPs target clients and then communicate with them for the provision of their services in certain languages, it is fair that clients are informed of their rights also in a language that they can understand.
59. In addition, also due to the digital and cross-border nature of the services provided, CASPs may easily target and reach retail clients (through social media, for instance...). Filing (i.e. drafting) a complaint requires a more advanced level of knowledge of a language than the level of understanding required to understand marketing communications or a template for filing complaints. For this reason, it is important to make sure that, for each Member State in which a CASP operates, it accepts complaints filed i) in the languages used by the CASP to market its services or communicate with clients in such Member State as well as ii) in the official languages of such Member State that are also official languages of the Union.
60. Whilst such requirements may appear as burdensome, ESMA is of the view that artificial intelligence and automated translation tools may help greatly reduce the costs associated. In view also of the objectives and issues at stake, ESMA deems such requirements as proportional.
61. Therefore, Option 2b has been chosen as the preferred option.

### [Policy issue 3: Publication of the description of the complaints-handling procedures and template](#)

62. Article 71(1) of MiCA provides that CASPs shall publish descriptions of their complaints-handling procedures. In this context, ESMA considered two policy options:
  - Option 3a. Remain silent in this draft RTS and rely solely on the publication requirement in Article 71(1) of MiCA;
  - Option 3b. Indicate how and where CASPs should proceed to the publication.
63. The purpose of the publication requirement in Article 71(1) of MiCA are to ensure that clients of a CASP can easily find the relevant information necessary to file a complaint. If the description of the complaints-handling procedures is not easily accessible by the clients, the purpose of the publication obligation under Article 72(5) would be defeated.



64. In addition, ESMA consider that Option 3b does not add any cost to those already ensuing from the level 1 text.
65. For these reasons, Option 3b has been chosen as the preferred option.

#### Policy issue 4: Resources dedicated to complaints-handling

66. To ensure the prompt, fair and consistent handling of complaints, the draft RTS provides that CASPs shall dedicate adequate resources to the management of complaints. ESMA considered the following two policy options in this respect:
- Option 4a. Remain silent on the topic.
  - Option 4b. Require that adequate resources be dedicated to the management of complaints.
  - Option 4c. Require adequate resources allocated to a separate complaints management function.
67. ESMA believes that Option 4a was running the risk that, without any clear requirement in this respect, CASP may not dedicate sufficient and appropriate resources to the management of complaints, thereby undermining the objective of Article 71 of MiCA (the prompt, fair and consistent handling of complaints).
68. To allow CASPs to adjust their internal organisation in light of the proportionality principle, ESMA chose not to require a separate complaints management function in all cases (option 5c). It is thus for each CASP to decide, based on the range of crypto-asset services provided and the scale of their activities, whether a separate complaints management function is necessary.
69. However, CASPs shall always ensure that the (human, financial and technical) resources dedicated to the management of complaints are adequate so that they can meet their obligations under Article 71, in particular the prompt, fair and consistent handling of complaints.
70. For these reasons, Option 4b has been chosen as the preferred option.

#### Policy issue 5: Maximum handling time of complaints

71. To ensure the prompt handling of complaints by CASPs, CASPs need to include the timeline applicable to the handling of a complaint in their complaints-handling procedures. To make sure that such timeline is not unreasonable, ESMA considered the following two policy options.

- Option 5a. Include in the draft RTS an obligation for CASPs to communicate their decision “as soon as possible” or “within a reasonable period”, without defining in the draft RTS a specific deadline.
  - Option 5b. Include in the draft RTS a specific deadline for CASPs to communicate their decision to the complainant after the receipt of the complaint.
72. Option 5a gave more flexibility to CASPs but also more uncertainty for clients of CASPs. It was also likely that different CASPs and different competent authorities would take different interpretations as to what should be considered “a reasonable period” or “as soon as possible”.
73. Option 5b, although more stringent, brings more certainty and more harmonisation. Given that the business model is almost exclusively digital, no delay in the communication CASP-client (unless due to the internal organisation of the CASP) is to be expected.
74. A definite deadline like the one provided in the draft RTS also gives CASPs a criteria to assess whether their handling of complaints is efficient. If they find that they are not able to comply with the two-months period provided in Article 6 of the draft RTS, it is likely that the complaints-handling procedures or resources allocated to the management of complaints need to be reviewed.
75. The deadline was set at two months as it was considered as giving sufficient time for CASPs to gather any necessary information and take a decision, whilst also being reasonable for clients awaiting a response from the CASP for the issue raised (which may involve significant financial repercussions for that client).
76. For these reasons, Option 5b was chosen as the preferred option.

#### *Cost-benefit analysis*

77. The RTS on complaints handling by CASPs are expected to bring both costs and benefits to the CASPs and competent authorities.

#### *Costs*

78. The main costs that CASPs are likely to incur stem from (i) the initial one-off costs related to the development of complaint handling procedures, the publication of the description of such procedures in the required languages and the setting up of adequate resources to manage complaints and (ii) the ongoing costs of ensuring compliance with the various requirements related to the receipt, investigation and response to complaints from clients as well as the analysis of complaints handling.

79. In terms of benefits, the clients of CASPs will be able to i) easily find and understand the information on how to submit their complaint and ii) benefit from a harmonised approach by CASPs to complaints-handling. This should result in increasing clients' confidence in CASPs and thus also benefit directly CASPs themselves.
80. It should be preliminary observed that since the requirements on complaints handling by CASPs are provided under MiCA, the impact of the draft RTS should be considered having in mind those legal provisions that they specify.

#### *Benefits*

81. Having harmonised complaints handling requirements regarding CASPs' complaints handling procedures, client information about complaints-handling, the template made available to clients to file a complaint, record-keeping of complaints and complaints-handling measures as well as CASPs' investigations of and responses to complaints will provide clients of CASPs across the Union with common and understandable information on the complaints- handling process and a uniform way for clients to submit complaints to CASPs. This will help ensure that complaints are treated in a fair, independent and harmonised way by CASPs.
82. Considering what has been illustrated above, ESMA believes that the overall costs associated with the implementation of the complaints-handling requirements set out in the draft RTS are fully justified by the objectives described above.

Table: Costs and benefits of the draft RTS in relation complaints-handling by CASPs

Stakeholder groups affected	Costs	Benefits
<b>CASPs</b>	<p>Initial one-off costs related to the development of complaints-handling procedures, the publication of the description of such procedures in the required languages and the setting up of adequate resources to manage complaints.</p> <p>Ongoing costs of ensuring compliance with the various requirements related to the receipt, investigation and response to complaints from clients in the required languages, as well as the ongoing analysis of complaints-handling data and (at least) annual review of the complaints-handling procedures by CASPs</p>	<p>Increasing the confidence that clients have in CASPs.</p> <p>Less reputational risk.</p> <p>Same regulatory burdens for all CASP no matter in which Member State they are registered.</p>
<b>Competent authorities</b>	Ongoing cost of supervision of complaints-handling by CASPs.	<p>Safer crypto-asset market.</p> <p>Less consumer complaints due to a better and harmonized handling of complaints.</p>
<b>Clients of CASPs</b>	None	<p>Able to rely on an EU-wide approach to complaints-handling by CASPs with i) easy access to the relevant information, ii) the possibility to get such information and file their complaint in a language that is understandable and iii) the prompt (maximum 2 months), fair and consistent handling of their complaint.</p>

## 6.1.4 RTS in relation to intended acquisitions of a qualifying holding in a CASP

### *Impact of the draft RTS under Article 84 (4) of MiCA*

83. Pursuant to Article 10(1) of Regulation (EU) No 1095/2010, 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.
84. MiCA requires natural or legal persons or such persons acting in concert who have taken a decision either to acquire, directly or indirectly a qualifying holding in a CASP or to increase, directly or indirectly, such a qualifying holding so that the proportion of the voting rights or of the capital held would reach or exceed 20 %, 30 % or 50 % or so that the CASP would become its subsidiary, to notify the competent authority of that CASP in writing indicating the size of the intended holding and the information allowing the national competent authority to assess all the following: the reputation of the proposed acquirer; the reputation, knowledge, skills and experience of any person who will direct the business of the crypto-asset service provider as a result of the proposed acquisition; the financial soundness of the proposed acquirer, in particular in relation to the type of business envisaged and pursued in respect of the crypto-asset service provider in which the acquisition is proposed; whether the crypto-asset service provider will be able to comply and continue to comply with the relevant provisions of MiCA; whether there are reasonable grounds to suspect that, in connection with the proposed acquisition, money laundering or terrorist financing within the meaning of, respectively, Article 1(3) and (5) of Directive (EU) 2015/849 is being or has been committed or attempted, or that the proposed acquisition could increase that risk.
85. The next paragraphs present the cost benefit analysis of the main policy options included in this final report on the detailed content of the information that is necessary to carry out the assessment referred to in Article 84 of MiCA.

### *Problem identification*

86. The notification about the proposed acquisition of a qualifying holding in a CASP to the competent authority must include all the information set out in the RTS specifying the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a CASP, with the appropriate level of detail to enable the competent authority to carry out the assessment of the criteria set out in Article 84 (1) of MiCA.
87. Lack of standardised information in the notification for the assessment of a proposed acquisition of a qualifying holding in a CASP would lead to diverging approaches and

different practices across Member States, hindering the level playing field and leading to regulatory arbitrage across EU Member States. Against this background, MiCA mandates ESMA, in close cooperation with the EBA, to develop an RTS to specify the detailed content of the information that is necessary for NCAs to carry out the assessment of the proposed acquirer of a qualifying holding in a CASP.

88. In addition, by assessing natural or legal persons proposing to acquire a qualifying holding in a CASP, competent authorities provide a safer market in crypto asset and a safer space for investors in crypto assets, despite the risks that any investment in crypto-assets represents.

#### *Policy objectives*

89. The strategic objective of the draft RTS is to harmonise the detailed information that proposed acquirers must submit to NCAs when proposing to acquire a qualifying holding in a CASP.

#### *Baseline scenario*

90. The baseline scenario is the situation where proposed acquirers of qualifying holdings in CASP must comply with their obligations under Article 83 of MiCA, of notifying NCAs of their intention to acquire a qualifying holding in a CASP without any further specification of these requirements by any draft RTS. Thus, competent authorities would request information from proposed acquirers to inform their assessments based on the criteria set out in Article 84 (4) of MiCA.
91. This may have a twofold significant impact. Firstly, the information contained in the notifications would be rather high-level and lack appropriate detail. This may not enable competent authorities to swiftly and effectively assess whether the proposed acquirer is of sufficient good repute, knowledgeable and sufficiently sound from a financial perspective.
92. Secondly, the information requested by competent authorities may diverge significantly across Member States. This may result in competent authorities taking diverging approaches to assess proposed acquirers. This can lead to regulatory arbitrage between Member States, with proposed acquirers opting for CASPs based in jurisdictions where competent authorities have a more permissive approach to the assessment of their reputation.

#### *Options considered and preferred options*

93. This section presents the main policy options discussed and the decisions made when developing the draft RTS. The policy options' respective advantages and disadvantages and the preferred options resulting from this analysis are assessed below.

## Policy issue 1: Level of detail of the information required to assess proposed acquirers of qualifying holdings in CASPs

94. ESMA considered two policy options:

- Option a: Set out high-level requirements in the draft RTS for the information to be included in the notification from the proposed acquirer.
- Option b: Include detailed information in the RTS which would be in line with existing regulatory frameworks on the assessment of proposed acquisitions of qualifying holdings in other types of regulated entities (e.g. investment firms).

95. The assessment of the proposed acquisition by the national competent authority must be based on the following criteria according to MiCA: the reputation of the proposed acquirer; the reputation, knowledge, skills and experience of any person who will direct the business of the crypto-asset service provider as a result of the proposed acquisition; the financial soundness of the proposed acquirer, in particular in relation to the type of business envisaged and pursued in respect of the crypto-asset service provider in which the acquisition is proposed; whether the crypto-asset service provider will be able to comply and continue to comply with the relevant provisions of MiCA; whether there are reasonable grounds to suspect that, in connection with the proposed acquisition, money laundering or terrorist financing within the meaning of, respectively, Article 1(3) and (5) of Directive (EU) 2015/849 is being or has been committed or attempted, or that the proposed acquisition could increase the risk thereof. Option a would allow to further specify some of the information required for competent authorities to assess those criteria, however, it could lead to competent authorities requesting additional information from proposed acquirers to ensure that the criteria mentioned in MiCA are met. This may cause inefficiencies in the assessment process, could lead to divergent approaches among competent authorities and eventually to regulatory arbitrage, increasing the risk that natural or legal persons with qualifying holdings in CASPs (and therefore influence in the business of the CASPs) would not be of sufficiently good repute. This could contribute to mistrust in markets in crypto assets and risks to investors.

96. To allow a competent authority to have the information necessary to meaningfully assess a proposed acquirer of a qualifying holding in a CASP, the notification should include sufficiently detailed information, in line with regulatory requirements already applying to proposed acquirers of qualifying holdings in other types of regulated entities (e.g. investment firms). Furthermore, considering the specificities of the business of CASPs, the detailed information provided by proposed acquirers of qualifying holdings in CASPs should be tailored in some instances (e.g. regarding the level of knowledge and experience of the proposed acquirer on crypto-assets and matters related to digital innovation).

97. Thus, Option b was chosen as the preferred option.

### *Cost-benefit analysis*

98. The draft RTS specifying the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a CASP is expected to result in both costs and benefits to proposed acquirers and competent authorities.

### *Costs*

99. Proposed acquirers will mostly incur one-off costs related to the collection of data and the preparation of the notification.
100. For competent authorities, the costs relate to the resources required for the assessment of the notification by proposed acquirers. Considering that the assessment of proposed acquisitions of qualifying holdings is a requirement which already exists for certain regulated entities, it is to be expected that NCAs responsible for the authorisation and supervision of those regulated entities (e.g. investment firms) already have in place procedures for the assessment of qualifying holdings which can be replicated or used in the case of CASPs.
101. Considering the requirements on the notification by proposed acquirers of qualifying holdings provided under MiCA, the impact of the draft RTS should be considered having in mind those legal provisions that they specify and the legal mandate on which they are based.

### *Benefits*

102. In terms of benefits, the draft RTS promote convergence and foster clarity and predictability for proposed acquirers of qualifying holdings in CASPs. The harmonised application requirements also promote fair competition between CASPs and a safer environment for investors in crypto assets, no matter the Member State where the CASP has been authorised.



*Table: Costs and benefits of the draft RTS specifying the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a CASP*

Stakeholder groups affected	Costs	Benefits
Proposed acquirer	Initial one-off costs to gather the required information and prepare the notification and sending it to the relevant competent authority.	Clarity and predictability of the information required for notification. Level-playing field.
Competent authorities	Initial one-off costs to adapt internal process for the assessment of notifications related to the proposed acquisition of a qualifying holding in a CASP.  Ongoing costs to assess the notifications.	Harmonisation and level-playing field. Clarity on the necessary level of detail required in notifications.

## 6.2 Annex II – Advice of the Securities and Markets Stakeholder Group

# Advice to ESMA

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

#### **1 Executive summary**

The rise of crypto assets in the last few years – through ‘boom and bust’ cycles that are common in unregulated settings – highlights the potential of an innovation that may transform the financial system but also poses investor protection issues. The SMSG believes that regulation in this area should balance the need for investor protection with the need to create an environment that does not stifle innovation.

The SMSG also considers that entities active in the crypto space should be subject to the same regulation and oversight as intermediaries providing economically equivalent financial services. This is the case not only for reasons related to level playing field but indeed to insure financial stability and investor protection. In the long run, a sound regulatory framework coupled with a rigorous oversight would promote trust in the user base and ultimately the growth of the crypto ecosystem.

The ‘two-track approach’ (i.e., notification requirements for regulated financial entities largely following the authorisation requirements for other entities, without mirroring them fully) is understandable and appropriate. The SMSG welcomes the alleviated notification regime granted to the most highly regulated players, based on the assumption that such entities are considered generally suitable to provide crypto-assets services. The Advice provides some suggestions on specific aspects. For example, as crypto assets are not covered by Investors Compensation Schemes (ICSs), the SMSG suggests enriching the information package submitted to NCAs to explain the measures that will be put in place to make retail clients aware of the different levels of asset protection.

ESMA has identified various undesirable developments in the crypto ecosystem, some of which have led to the collapse of crypto-asset service providers, drawing lessons from these events. ESMA takes these undesirable developments into account in the definition of the information to be submitted with the application. The SMSG welcomes this approach, which seems necessary in the interest of effective investor protection.

The SMSG believes that the online marketing activity performed by so-called ‘Finfluencers’ deserves to be considered as it is a prominent aspect of the distribution of crypto assets and may lead to potential cases of false advertisements and price manipulation.

The SMSG welcomes the clarification from ESMA that conflicts of interests should either be prevented or managed, and the disclosure requirements are not an alternative to the prevention or management of conflicts of interests. The SMSG also believes that conflicts of interests should preferably be prevented, and managed only if prevention is not possible.

This Advice also provides the views of the Group on some general aspects related to the regulation of crypto-assets, based on the understanding that MiCA is designed as a building-block of a wider regulatory effort, which includes initiatives such as the Digital Operational Resilience Act (DORA), the DLT Pilot Regime and the Transfer of Funds Regulation (TFR).

As crypto markets are intrinsically global in nature, the SMSG highlights the need to have a cross-border coordinated approach to foster investor protection and minimize regulatory arbitrage. Cryptos amplify the need to clarify what conduct qualifies for solicitation or reverse solicitation due to the existence of multiple crypto-specific channels to approach clients like blogs and message boards.

MiCA Regulation is an entity-based set of rules. However, financial services may also be provided through Decentralized Finance (DeFi) settings. The SMSG understands that MiCA requires an assessment of the development of DeFi in markets in crypto-assets and of the necessity and feasibility of regulating DeFi by 30 December 2024. The SMSG highlights the need to start immediately monitoring the developments in the DeFi area and offering clarifications as to whether the MiCA Regulation applies to specific operations performed in a DeFi setting.

While MiCA Regulation provides fundamental safeguards, the SMSG also believes that investors should be in a position not to overrate the protection provided by MiCA. The SMSG considers that it would be useful to monitor the use that crypto-asset service providers make of the MiCA authorisation in their communication.

## 2 Background

1. On 20 July 2023, ESMA released the first MiCA consultation package as part of a series of three packages that will be published sequentially. This first consultation package covers the following aspects:
  - i. the notification by certain financial entities of their intention to provide crypto-asset services;
  - ii. the authorisation of crypto-asset service providers (CASPs);
  - iii. complaints handling by CASPs;
  - iv. the identification, prevention, management and disclosure of conflicts of interests by CASPs;
  - v. the proposed acquisition of a qualifying holding in a CASP.

2. Additionally, in the last part of the paper – as this is the first public consultation following the publication of the final text of MiCA – ESMA asks for insights on key general aspects concerning entities that plan to offer services in EU jurisdiction(s) falling under the scope of MiCA. While the SMSG is not able to provide inputs in this respect, the Group still tries to contribute to the consultation process with some elements related to the regulation of crypto-assets.
3. The rise of crypto assets in the last few years – through ‘boom and bust’ cycles that are common in unregulated settings – highlights the potential of an innovation that may transform the financial system but also poses investor protection issues. The SMSG believes that regulation in this area should balance the need for investor protection with the need to create an environment that does not stifle innovation.
4. The SMSG also believes that entities active in the crypto space should be subject to the same regulation and oversight as intermediaries providing economically equivalent financial services. This is the case not only for reasons related to level playing field but indeed to insure financial stability and investor protection. In the long run, a sound regulatory framework coupled with a rigorous oversight would promote trust in the user base and ultimately the growth of the crypto ecosystem.
5. The SMSG understands that other topics – like market abuse or the qualification of crypto-assets as financial instruments – will be dealt with in the next consultation packages. Consequently, this Advice will not discuss such topics.
6. The rest of the Advice is organised as follows. Section 3 provides comments on aspects included in the draft RTS and ITS, listed in § 1, and Section 4 discusses other aspects that – although not included in the consultation paper – are relevant for the regulation of crypto-asset markets.

### **3 Comments on aspects included in the drafts RTS and ITS**

7. As a general and preliminary remark, the SMSG notes that the Level 1 text and the related delegations provide a detailed framework, leaving limited room for changes.

#### **3.1 Provision of crypto-asset services by certain financial entities: A notification procedure**

8. MiCA provides that entities that already have a license to provide financial services and that already went through the authorisation process with the NCA of their home Member State (such as investment firms, credit institutions, etc.), do not need to go through the entire authorisation process again. Such entities are required to notify their relevant NCA that they intend to provide crypto-asset services, including the specific information relevant to the provision of such services.

9. The SMSG welcomes the alleviated notification regime granted to the most highly regulated players, based on the assumption that such entities are considered generally suitable to provide crypto-assets services.
10. In addition, the ‘two-track approach’ (i.e., notification requirements for regulated financial entities largely following the authorisation requirements for other entities, without mirroring them fully) is understandable and appropriate. For instance, if relevant information was already available to the NCA and the provision of crypto-asset services did not require any changes in the organisational structure, this information would not have to be submitted again. Tangible relief for notifying future CASPs could result, for example, from the fact that, unlike in the authorisation procedure, evidence of a sufficiently good reputation and appropriate knowledge, skills and experience of the business managers do not have to be provided again. Furthermore, it does not seem strictly necessary to impose the preparation of a detailed business plan for the following 3 years (Art. 1 of the draft RTS on the notification by certain financial entities) as well as extensive presentations on the IT concept and IT security (Art. 4 of the draft RTS on the notification by certain financial entities) on regulated companies that want to provide only, e.g., the services of investment advice, investment brokerage or portfolio management.
11. The likely development over time of new types of crypto-assets which were not yet known at the time of notification raises a point. Article 7 of the draft RTS on the notification by certain financial entities (Section 9.2.1) provides that the notifying entity should specify, among other things, which types of crypto-assets will not be admitted to trading on its platform and the reasons for this. It would be helpful to provide details regarding the procedure of potential future update and the meaning associated to the wording “types of crypto-assets” (e.g., whether it is sufficient to refer to the three types of crypto-assets defined by Article 3 of MiCA, ‘asset-referenced tokens’ vs. ‘e-money tokens’ vs. ‘utility token’).
12. In the context of the description of the trading system and market abuse surveillance (Art. 7 of the draft RTS on the notification by certain financial entities, Section 9.2.1), it should be described whether the final settlement of transactions is initiated on the Distributed Ledger Technology (DLT) or outside the DLT. Additionally, a notifying entity intending to operate a trading platform for crypto-assets shall provide to the NCA the definition of the moment at which settlement is final (Article 7, § 1 (k) (vi)). In this respect, standardization or self-regulation may prevail. In the first option, the Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality is already in force for the traditional securities settlement systems, and would serve well the purpose of standardization. However, by nature, it does not deal yet with crypto-assets and their settlement. The second option may be preferred for the sake of the frequently postulated openness to technology. The SMSG acknowledges this option and welcomes the possibility of adopting the preferred solution at the choice of the provider.

13. MiCA states that crypto assets are not covered by Investors Compensation Schemes (ICSs) under Directive 97/9/EC<sup>4</sup>. This provision creates a situation in which regulated entities like banks and investment firms will be providing the same service (i.e., custody or portfolio management) to the same retail clients and, however, only part of the relevant assets will be covered by an ICS in case of insolvency<sup>5</sup> of the institution while some other assets will not. This set up implies a change from the perspective of retail investors: an entity that was previously thought to be covered by an ICS will no longer be a covered entity for the full scope of the investments, as it will be a covered entity for some investments and not for others.
14. Against this background, the SMSG considers that possible investors disappointments and reputational issues may arise, leading to serious concerns on investors awareness and investors protection. The Group suggests to include – in the information package that a bank or an investment firm has to send to the NCA before providing services on crypto assets – an explanation of the measures that will be put in place in order (1) to make retail clients aware of the different levels of asset protection and (2) to let them know at all times what investments are protected by an ICS and what are not.

### **3.2 Provision of crypto-asset services by other entities: An authorisation regime**

15. ESMA has identified various undesirable developments in the crypto ecosystem, some of which have led to the collapse of CASPs, drawing lessons from these events. Specifically, ESMA criticised (i.) the lack of basic information on the corporate structure of the service provider and its financial resources, (ii.) the lack of transparency regarding the characteristics and scope of entities associated with the service provider, and (iii.) the offering of various services related to crypto-assets that were not subject to (sufficient) regulation and supervision.
16. ESMA takes these undesirable developments into account in the definition of the information to be submitted with the application. The SMSG welcomes this approach, which seems necessary in the interest of effective investor protection. This applies in particular to the measures for the segregation of clients' crypto-assets and funds (§ 39). For example, the lack of such measures was a major cause of the collapse of FTX, a case in which investors suffered considerable losses. Against this background, it looks reasonable that the information provided by a legal entity or other enterprise that intends to provide crypto-asset services in the future (Art. 62 MiCA) in order to apply for permission to the competent NCA should be more comprehensive than for a notification, as the NCA has to gather appropriate information.

---

<sup>4</sup> Articles 6, 19, 51 and 81 of MiCA.

<sup>5</sup> The term insolvency is used to express that the conditions required to compensate the investors are met in accordance with article 2.2. of Directive 97/9.

17. The SMSG believes that the online marketing activity performed by so-called 'Finfluencers' deserves to be considered as it is a prominent aspect of the distribution of crypto assets. Regulation and enforcement of rules and liabilities are required to protect investors and markets from false advertisements and price manipulation. Social media platforms should have an incentive to moderate the activity of Finfluencers, as they may cause damages to investors through incorrect assertions of facts. In the past, prominent figures have apparently used their fame to raise the prices of some crypto assets and then sell them, resembling classical "pump and dump" schemes which are illegal. It is important to ensure that these rules apply to crypto markets as well. On a general basis, the advices that are provided by Finfluencers should be regulated as the advices provided by financial advisors and monitored to control the spread of sharp practices in the dissemination of promotional information about crypto assets.

### **3.3 Complaints handling by crypto-asset service providers**

18. The SMSG understands that the approach adopted by ESMA is different from the one adopted by the EBA for its mandate under Article 31(5) of MiCA, regarding complaints-handling procedures for issuers.
19. The SMSG notes that it would be desirable that the rules on complaint management are uniform within a regulatory framework such as MiCA, as it can be assumed that some companies act both as issuers and as CASPs. Therefore, further harmonisation and standardisation of the rules on complaint management should be undertaken.

### **3.4 Conflicts of interests**

20. Article 72 of MiCA provides that crypto-asset service provider "shall implement and maintain effective policies and procedures [...] to identify, prevent, manage and disclose" conflicts of interest.
21. The consultation paper clarifies that conflicts of interests should either be prevented or managed and the disclosure requirements of Article 72(1), as further detailed in paragraph 2 of Article 72, are not an alternative to the prevention or management of conflicts of interests. The SMSG welcomes this clarification from ESMA. Additionally, the SMSG believes that conflicts of interests should preferably be prevented, and managed only if prevention is not possible.
22. The SMSG welcomes that ESMA has closely followed the Delegated Regulation on MiFiD II on conflicts of interests. Other regulatory frameworks would have indeed resulted with overburdening the financial institutions that are already regulated under MiFiD.



## 4 Other aspects

23. The SMSG understands that MiCA is designed as a building-block of a wider regulatory effort, which includes initiatives such as the Digital Operational Resilience Act (DORA), the DLT Pilot Regime and the Transfer of Funds Regulation (TFR). The SMSG is aware of the possibility that some of the points that are raised in this opinion might imply changes at Level 1 or require the involvement of other ESAs or be covered in other parts of the EU's overarching initiative to regulate digital assets. Still, it is deemed as potentially useful to share the SMSG view on these points.

### 4.1 Non-EU entities and cross-border crypto-asset services

24. Crypto markets are intrinsically global in nature. Investors located in the EU might have access to crypto-assets regulated in different jurisdictions. Several exchanges are located in other jurisdictions. To protect EU investors, the challenge is to bring crypto services into the scope of EU regulation when EU citizens are involved. The SMSG highlights the need to have a cross-border coordinated approach to foster investor protection and minimize regulatory arbitrage.
25. MiCA waives the requirement for authorisation where an EU client initiates at its own exclusive initiative the provision of crypto-asset services ('reverse solicitation', Article 61.1). Paragraph 2 of Article 61 clarifies that the client's own initiative does not entitle a thirdcountry firm to 'market' new types of crypto-assets or crypto-assets services to that client. However, there is legal uncertainty as to the boundaries of reverse solicitation and there is a risk of solicitation cloaked as reverse solicitation.
26. Although the discussion on the boundaries of reverse solicitation is not unique to the crypto ecosystem, the SMSG highlights that cryptos amplify the need to clarify what conduct qualifies for solicitation or reverse solicitation due to the existence of multiple cryptospecific channels to approach clients like blogs, message boards, newsletters, referral programmes and partnership programmes.

### 4.2 Decentralized finance

27. MiCA Regulation is an entity-based set of rules (e.g., the CASP authorisation process or the CASP conflicts of interests). However, financial services may also be provided through decentralized applications running on permissionless networks like Ethereum with minimal or no intermediaries' involvement. This setting is usually referred to as Decentralized Finance (DeFi)<sup>6</sup>.

---

<sup>6</sup> Decentralized applications (or "protocols") are set of smart contracts which do not need to be operated by a clearly identifiable corporate entity. Developers may create and distribute governance tokens, which confer rights – e.g. related to the governance of the protocol – to their owners, to be exercised within novel forms of organization such as Decentralized Autonomous Organizations (DAOs). Decentralized finance emerges when the protocols provide users with financial services on a decentralized network.

28. The SMSG understands that, based on Article 142 of MiCA Regulation, by 30 December 2024 and after consulting EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the latest developments with respect to cryptoassets, including an assessment of the development of DeFi in markets in crypto-assets and of the necessity and feasibility of regulating DeFi<sup>7</sup>.
29. Given the dynamic nature of these technologies and the semantic difficulties associated with the interpretation of the related concepts, the SMSG highlights the need to start immediately monitoring the developments in the DeFi area and offering clarifications as to whether the MiCA Regulation applies to specific operations performed in a DeFi setting. Recital 22 of MiCA states that partially decentralized services are in scope of MiCA, whereas fully decentralized services in crypto-assets are not in MiCA scope<sup>8</sup>. However, ascertain whether a service is provided in a partially decentralised manner or in a fully decentralised manner is not straightforward<sup>9</sup>. Additionally, the risk of malpractices is present with decentralisation as well. For example, when decentralized applications act as market makers (i.e., Automated Market-Makers, AMMs) the underlying code should be made available to regulators for possible scrutiny in order to prevent market abuse.

### 4.3 Risk of misunderstanding MiCA scope and implications

30. MiCA Regulation provides operational, organisational and prudential requirements at Union level applicable to crypto-asset service providers to address potential risks that the provision of crypto-asset services poses to investor protection.
31. While MiCA Regulation provides fundamental safeguards, the SMSG also believes that investors should be in a position not to overrate the protection provided by MiCA. The no-endorsement statement<sup>10</sup> on the first page of the crypto-asset white paper is fully consistent with this approach.
32. Along the same lines, the SMSG believes that it would be useful to monitor the use that CASPs make of the MiCA authorisation in their communication. A potential risk is in the

---

<sup>7</sup> MiCA requires that the report is also expected to contain an assessment of the necessity (and feasibility) of regulating lending and borrowing of crypto-assets, an assessment of the treatment of e-money tokens, where not addressed in the review of the Payment Services Directive (PSD2), an assessment of the development of markets in non-fungible crypto-assets (e.g., NonFungible Tokens, NFTs) and of the appropriate regulatory treatment of such crypto-assets.

<sup>8</sup> 'This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation.'

<sup>9</sup> Even where crypto platforms pose as DeFi *stricto sensu*, it is far from certain whether they are, in fact, fully decentralized in MiCA's sense. Some type of legal entity is often related to fully decentralized platforms. See Zetzsche/Buckley/Arner/van Ek, *Remaining regulatory challenges in digital finance and crypto-assets after MiCA*, publication for the Committee on Economic and Monetary Affairs (ECON), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, May 2023. This document is available on the internet at: <http://www.europarl.europa.eu/supporting-analyses>.

<sup>10</sup> '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' (Articles 6(39 and 51(3)).

misuse of the authorisation received by NCAs to convey the idea that the crypto-assets are less risky thanks to this authorisation.

#### **4.4 Market stability and prudential requirements of CASPs**

33. MiCA provides prudential and conduct requirements for CASPs, including back-up systems and risk controls. The MSG notes that such requirements address the resilience of CASPs while a different – although interconnected – dimension of market stability refers to excessive volatility. This second dimension also deserves attention, for investor protection purposes and market abuse prevention, as issuers may limit the supply, pushing upwards the market price for the crypto asset. This practice - which essentially leads to ‘positioning’ the market price at an artificial level - is similar to a market corner or squeeze.
34. With respect to prudential requirements, the MSG understands that the introduction of a prudential regime for CASPs is intended to ensure consumer protection (Recital 80). To create a level playing field between CASPs and regulated financial entities, prudential requirements should be subject to a test of functional equivalence, namely they should be similar to those of regulated institutions undertaking same functions.
35. According to Article 67 of MiCA, CASP shall have prudential safeguards equal to an amount of at least the higher of the following two items: an amount of permanent minimum capital requirements – that ranges from EUR 50,000 to EUR 150,000 depending on the type of the crypto-asset services provided – and 25% of the fixed overheads<sup>11</sup>.
36. While the MSG understands that prudential safeguards have been set by the Level 1 text and prudential regulation is not explicitly in ESMA remit, the MSG notes that prudential requirements – which may have an impact on market stability – do not appear to be fully related to the potential riskiness of CASPs as they do not take into account, e.g., the value of the assets in custody or the value of the crypto-assets placed or traded<sup>12</sup>.

---

<sup>11</sup> The prudential safeguards may be complied with own funds of the CASP or an insurance policy.

<sup>12</sup> Annex IV of MiCA provides minimum capital requirements for CASPs offering, among others, execution of orders on behalf of clients, providing custody and administration of crypto-assets on behalf of clients, exchange of crypto-assets for fund, operation of a trading platform for crypto-assets. The exchange of crypto assets for funds, as defined by Article 3.1.(19), is a market making activity where the CASP buys and sells contracts concerning crypto-assets with clients for funds by using proprietary capital.

## 6.3 Annex III – Draft RTS pursuant to Article 60(13) 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 information to be included in a notification by certain financial entities of their intention to provide crypto-asset services**

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>13</sup>, and in particular Article 60(13), third subparagraph, thereof,

Whereas:

- (1) The information to be provided in a notification by certain financial entities of their intention to provide crypto-asset services should be sufficiently detailed and comprehensive to enable competent authorities to assess whether the notifying entity meets the applicable requirements laid down in Title V and, where relevant, Title VI of Regulation (EU) 2023/1114.
- (2) A notification to provide crypto-asset services should contain a programme of operations, describing the notifying entity's organisational structure, strategy in providing crypto-asset services to its targeted clients, and its operational capacity for the three years following notification. Where describing the strategy used to target clients, the notifying entity should describe the marketing means that it intends to use such as, for instance, websites, mobile phone applications, face-to-face meetings, press releases, or any form of physical or electronic means, including social media campaign tools, internet advertisements or banners, retargeting of advertising, agreements with influencers, sponsorships agreements, calls, webinars, any invitation to an event, affiliation campaign, gamification techniques, invitation to fill in a response form or to follow a training course, demo accounts or educational materials.
- (3) The competent authority should be able to assess the notifying entity's resilience to withstand external financial shocks, including those concerning the value of crypto-assets. Therefore, the notifying entity should include stress scenarios simulating severe but plausible events in its forecast accounting plan.

---

<sup>13</sup>OJ L 150, 9.6.2023, p. 40.

- (4) In the financial services system, time is often of the essence. It is thus critical to maintain operations or at least essential functions and to minimise downtime due to unexpected disruptions (such as cyberattacks, natural disasters) to avoid outages as they can have major financial, regulatory and reputational consequences for the notifying entity and crypto-assets markets more generally. A notification should thus contain detailed information on the notifying entity's arrangements to ensure continuity and regularity in the performance of its crypto-asset services, including a detailed description of its business continuity and disaster recovery plans.
- (5) Effective mechanisms, systems and policies and procedures in compliance with Directive (EU) 2015/849 of the European Parliament and of the Council<sup>14</sup> are crucial to ensure that notifying entities appropriately address risks and practices of money laundering and terrorist financing in the provision of crypto-asset services. Thus, notifying entities should provide detailed information on their mechanisms, systems and policies and procedures on how they prevent, inter alia, anti-money laundering and counter-terrorist financing risks associated with their business activities.
- (6) Due to the decentralised and digital nature of crypto-assets, cybersecurity risks for crypto-asset service providers are significant and take many forms. To ensure that applicants are able to prevent data breaches and financial losses that may be caused by cyberattacks, competent authorities should be provided with information on the applicants' deployed ICT systems and related security arrangements, including the human resources dedicated to addressing cybersecurity risks.
- (7) The segregation of client crypto-assets and funds is an important part of the regime regulating crypto-asset services as it protects clients from losses of the crypto-asset service provider and from misuse of their crypto-assets and funds. Crypto-asset service providers are therefore subject to an obligation to make adequate arrangements to safeguard clients' ownership rights. This requirement also applies to crypto-asset service providers which do not provide custody and administration services.
- (8) To allow national competent authorities to assess the adequacy of the notifying entity's operating rules of trading platforms for crypto-assets, specific elements should be detailed in their description. In particular, the notifying entity should elaborate aspects of the operating rules relating to the admission to trading of crypto-assets, the trading and the settlement of crypto-assets. Relating to the admission to trading, notifying entities should provide detailed information on rules governing the admission of crypto-assets to trading, the way in which the admitted crypto-assets comply with the notifying entity's rules, the types of crypto-assets that the notifying entity will not admit to its platform and the reasons for these exclusions and fees applicable to the admission to trading. As for the trading of crypto-assets, the notifying entity should further specify in the description of the operating rules, the elements of those rules which govern the execution and cancellation of orders, elements which aim at ensuring orderly trading and transparency and record-keeping rules. Finally, the notifying entity should include in the description of the operating rules the elements governing the settlement of transactions of crypto-assets concluded on the trading platform, including whether the settlement of

---

<sup>14</sup> Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

transactions is initiated in the Distributed Ledger Technology (DLT), the timeframe in which the execution is initiated, the definition of the moment at which the settlement is final, all verifications required to ensure the effective settlement of the transaction and any measure in place to limit settlement failures.

- (9) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority (ESMA) to the European Commission, as developed in close cooperation with the European Banking Authority (EBA).
- (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 of the European Parliament and of the Council<sup>15</sup>,

HAS ADOPTED THIS REGULATION:

#### *Article 1*

#### **Programme of operations**

1. A notifying entity shall provide to the competent authority the programme of operations for the following three years, including all of the following information:

- (a) where the notifying entity belongs to a group, an explanation of how the activities of the notifying entity will fit within the group strategy and interact with the activities of the other entities of the group, including an overview of the current and planned organisation and structure of the group;
- (b) an explanation of how the activities of the entities affiliated with the notifying entity, including where there are regulated entities in the group, is expected to impact the activities of the notifying entity. This explanation shall include a list of and information on the entities affiliated with the notifying entity, including where there are regulated entities, the services provided by these entities (including regulated services, activities and types of clients) and the domain names of each website operated by such entities;
- (c) a list of crypto-asset services that the notifying entity intends to provide as well as the types of crypto-assets to which the crypto-asset services will relate;

---

<sup>15</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).



- (d) other planned activities, regulated in accordance with Union or national law or unregulated, including any other services, than crypto-asset services, that the notifying entity intends to provide;
- (e) whether the notifying entity intends to offer crypto-assets to the public or seek admission to trading of crypto-assets and if so, of what type of crypto-assets;
- (f) a list of jurisdictions, in and outside the European Union, in which the notifying entity plans to provide crypto-asset services, including information on the domicile of targeted clients and the targeted number by geographical area;
- (g) types of prospective clients targeted by the notifying entities' crypto-asset services;
- (h) a description of the means of access to the notifying entity's crypto-asset services by clients, including all of the following:
  - (i) the domain names for each website or other ICT-based application through which the crypto-asset services will be provided by the notifying entity and information on the languages in which the website will be available, the types of crypto-asset services that will be accessed through it and, where applicable, from which Member States the website will be accessible;
  - (ii) the name of any ICT-based application available to clients to access the crypto-asset services, in which languages it is available and which crypto-asset services can be accessed through it;
- (i) the planned marketing and promotional activities and arrangements for the crypto-asset services, including:
  - (i) all means of marketing to be used for each of the services, the means of identification that the notifying entity intends to use and information on the relevant category of clients targeted and types of crypto-assets;
  - (ii) languages that will be used for the marketing and promotional activities;
- (j) a detailed description of the human, financial and ICT resources allocated to the intended crypto-asset services as well as their geographical location;
- (k) the notifying entity's outsourcing policy and how it was adapted to crypto-asset services as well as a detailed description of the notifying entity's planned outsourcing arrangements, including intra-group arrangements, how the notifying entity intends to comply with the requirements set out in Article 73 of Regulation (EU) 2023/1114. The notifying entity shall also include information on the functions or person responsible for outsourcing, the resources (human and ICT) allocated to the control of the outsourced functions, services



or activities of the related arrangements and on the risk assessment related to the outsourcing;

- (l) the list of entities that will provide outsourced services for the provision of crypto-asset services, their geographical location and the relevant services outsourced;
- (m) a forecast accounting plan including stress scenarios at an individual and, where applicable, at consolidated group and sub-consolidated level in accordance with Directive 2013/34/EU. The financial forecast shall consider any intra-group loans granted or to be granted by and to the notifying entity;
- (n) any exchange of crypto-assets for funds and other crypto-asset activities that the notifying entity intends to undertake, including through any decentralised finance applications with which the notifying entity wishes to interact on its own account.

2. Where the notifying entity intends to provide the service of reception and transmission of orders for crypto-assets on behalf of clients, it shall provide to the competent authority a copy of the policies and procedures and a description of the arrangements ensuring compliance with the requirements set out in Article 80 of Regulation (EU) 2023/1114.

3. Where the notifying entity intends to provide the service of placing of crypto-assets, it shall provide to the competent authority a copy of the policies and procedures and a description of the arrangements in place to comply with Article 79 of Regulation (EU) 2023/1114 as well as Article 9 of [RTS on conflicts of interest of CASPs].

## *Article 2*

### **Business continuity**

1. A notifying entity shall submit to the competent authority a detailed description of the notifying entity's business continuity plan, including which steps shall be taken to ensure continuity and regularity in the performance of the notifying entity's crypto-asset services.

2. The description shall include details showing that the established business continuity plan is appropriate and that arrangements are set up to maintain and periodically test it. The description shall explain, with regard to critical or important functions supported by third-party service providers, how business continuity is ensured in the event that the quality of the provision of such functions deteriorates to an unacceptable level or fails. The description shall also explain how business continuity is ensured in the event of the death of a key person and, where relevant, political risks in the service provider's jurisdiction.

### *Article 3*

#### **Detection and prevention of money laundering and terrorist financing**

A notifying entity shall provide the competent authority with information on its internal control mechanisms and policies and procedures to ensure compliance with the provisions of national law transposing Directive (EU) 2015/849 and with information on the risk assessment framework to manage risks relating to money laundering and terrorist financing, including all of the following:

- (a) the notifying entity's assessment of the inherent and residual risks of money laundering and terrorist financing associated with its provision of crypto-asset services, including the risks relating to the notifying entity's customer base, to the services provided, to the distribution channels used and to the geographical areas of operation;
- (b) the measures that the notifying entity has or will put in place to prevent the identified risks and comply with applicable anti-money laundering and counter-terrorist financing requirements, including the notifying entity's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;
- (c) detailed information on how such mechanisms, systems and procedures are adequate and proportionate to the scale, nature, inherent money laundering and terrorist financing risk, range of crypto-asset services provided, the complexity of the business model and how they ensure the notifying entity's compliance with Directive (EU) 2015/849 and Regulation (EU) 2023/1113;
- (d) the identity of the person in charge of ensuring the notifying entity's compliance with anti-money laundering and counter-terrorist financing obligations, and evidence of the person's skills and expertise;
- (e) arrangements, human and financial resources devoted to ensure that staff of the notifying entity is appropriately trained in anti-money laundering and counter-terrorist financing matters (annual indications) and on specific crypto-asset related risks;
- (f) a copy of the notifying entity's anti-money laundering and counter-terrorism policies and procedures and systems;
- (g) a summary document outlining changes that have been made to the notifying entity's anti-money laundering and counter-terrorism policies and procedures and systems as a consequence of the planned crypto-asset services;
- (h) the frequency of the assessment of the adequacy and effectiveness of such mechanisms, systems and policies and procedures as well as the person or function responsible for such assessment.

*Article 4*

**ICT systems and related security arrangements**

A notifying entity shall submit to the competent authority all of the following information:

- (a) technical documentation of the ICT systems, on DLT infrastructure relied upon, where relevant, and on the security arrangements. The applicant shall include a description of the arrangements and deployed ICT and human resources established to ensure that the applicant complies with Regulation (EU) 2022/2554, including, but not limited to:
- (i) a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system, including a detailed description of ICT systems, protocols and tools and of how the applicant's procedures, policies and systems to safeguard the security, integrity, availability, authenticity and confidentiality of data in accordance with Regulation (EU) 2022/2554 and Regulation (EU) 2016/679;
  - (ii) an identification of ICT services supporting critical or important functions, developed or maintained by the applicant, as well as those provided by third-party service providers, a description of such contractual arrangements (identity and geographical location of the providers, description of the outsourced activities or ICT services with their main characteristics, copy of contractual agreements) and how they comply with Article 73 of Regulation (EU) 2023/1114 and the Chapter V of Regulation (EU) 2022/2554;
  - (iii) a description of the applicant's procedures, policies, arrangements and systems for security and incident management;
- (b) a cybersecurity audit realized by a third-party cybersecurity auditor having sufficient experience in accordance with [DORA TLPT RTS detailing the minimum requirements on capabilities which are described in DORA Level 1 Article 27] covering: the following audits or tests performed by external independent parties:
- (i) organisational cybersecurity, physical security and secure software development lifecycle arrangements;
  - (ii) vulnerability assessments and scans, network security assessments;
  - (iii) configuration reviews of ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554;

- (iv) penetration tests on the ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554, in accordance with all the following audit test approaches:
  - black box: the auditor has no information other than the IP addresses and URLs associated with the audited target. This phase is generally preceded by the discovery of information and the identification of the target by querying domain name system (DNS) services, scanning open ports, discovering the presence of filtering equipment, etc.;
  - grey box phase: auditors have the knowledge of a standard user of the information system (legitimate authentication, “standard” workstation, etc.). The identifiers can belong to different user profiles in order to test different privilege levels;
  - white box phase: auditors have as much technical information as possible (architecture, source code, telephone contacts, identifiers, etc.) before starting the analysis. They also have access to technical contacts related to the target.
- (v) if the applicant uses and/or develops smart-contracts, a cybersecurity source code review of them.
- (c) a description of conducted audits of the ICT systems including used DLT infrastructure and security arrangements;
- (d) a description of the relevant information set out in subparagraphs a) and b) in non-technical language of the information provided under points a) and b).

#### *Article 5*

### **Segregation of clients’ crypto-assets and funds**

1. Where the notifying entity intends to hold crypto-assets belonging to clients or the means of access to such crypto-assets, or clients’ funds (other than e-money tokens), the notifying entity shall provide to the competent authority a detailed description of its policies and procedures for the segregation of clients’ crypto-assets and funds, including all of the following:

- (a) how the notifying entity ensures that
  - (i) clients’ funds are not used for its own account;
  - (ii) crypto-assets belonging to the clients are not used for its own account;

- (iii) the wallets holding clients' crypto-assets are different from the notifying entity's own wallets;
- (b) a detailed description of the approval system for cryptographic keys and safeguarding of cryptographic keys (for instance, multi-signature wallets);
- (c) how the notifying entity segregates clients' crypto-assets, including from other clients' crypto-assets in the event of wallets containing crypto-assets of more than one client (omnibus accounts);
- (d) a description of the procedure to ensure that clients' funds (other than e-money tokens) are deposited with a central bank or a credit institution by the end of the business day following the day on which they were received and are held in an account separately identifiable from any accounts used to hold funds belonging to the notifying entity;
- (e) where the notifying entity does not intend to deposit funds with the relevant central bank, which factors the notifying entity is taking into account to select the credit institutions to deposit clients' funds, including the notifying entity's diversification policy, where available, and the frequency of review of the selection of credit institutions to deposit clients' funds;
- (f) how the notifying entity ensures that clients are informed in clear, concise and non-technical language about the key aspects of the notifying entity's systems and policies and procedures to comply with Article 70(1), (2) and (3) of Regulation (EU) 2023/1114.

2. In accordance with Article 70(5) of Regulation (EU) 2023/1114, crypto-asset service providers that are electronic money institutions or credit institutions shall only provide the information listed in paragraph 1 above in relation to the segregation of clients' crypto-assets.

#### *Article 6*

### **Custody and administration policy**

A notifying entity intending to provide the service of custody and administration of crypto-assets on behalf of clients shall provide to the competent authority all of the following information:

- (a) a description of the arrangements linked to the type or types of custody offered to clients, a copy of the notifying entity's standard agreement for the custody and administration of crypto-assets on behalf of clients as well as a copy of the summary of the custody policy made available to clients in accordance with Article 75(3) of Regulation (EU) 2023/1114;
- (b) the notifying entity's custody and administration policy, including a description of identified sources of operational and ICT risks for the safekeeping and control of the crypto-assets or the means of access to the crypto-assets of clients, together with:

- (i) the policies and procedures, and a description of, the arrangements to ensure compliance with Article 75(8) of Regulation (EU) 2023/1114;
  - (ii) the policies and procedures, and a description of the systems and controls, to manage those risks, including when the custody and administration of crypto-assets on behalf of clients is outsourced to a third party;
  - (iii) the policies and procedures relating to, and a description of, the systems to ensure the exercise of the rights attached to the crypto-assets by the clients;
  - (iv) the policies and procedures relating to, and a description of, the systems to ensure the return of crypto-assets or the means of access to the clients;
- (c) information on how the crypto-assets and the means of access to the crypto-assets of the clients are identified;
- (d) information on arrangements to minimise the risk of loss of crypto-assets or of means of access to crypto-assets;
- (e) where the crypto-asset service provider has delegated the provision of custody and administration of crypto-assets on behalf of clients to a third-party:
- (i) information on the identity of any third-party providing the service of custody and administration of crypto-assets and its status in accordance with Article 59 or Article 60 of Regulation (EU) 2023/1114;
  - (ii) a description of any functions relating to the custody and administration of crypto-assets delegated by the crypto-asset service provider, the list of any delegates and sub-delegates (as applicable) and any conflicts of interest that may arise from such a delegation;
  - (iii) a description of how the notifying entity intends to supervise the delegations or sub-delegations.

#### *Article 7*

#### **Operating rules of the trading platform and market abuse detection**

1. A notifying entity intending to operate a trading platform for crypto-assets shall provide to the competent authority a description of all of the following:

- (a) rules regarding the admission of crypto-assets to trading;

- (b) the approval process for admitting crypto-assets to trading, including the customer due diligence carried out in accordance with Directive (EU) 2015/849;
- (c) the list of any categories of crypto-assets that will not be admitted to trading and the description of the reasons for such exclusion;
- (d) the policies and procedures and fees for the admission to trading, together with a description, where relevant, of membership, rebates and the related conditions;
- (e) the rules governing order execution, including any cancellation procedures for executed orders and for disclosing such information to market participants;
- (f) the policies and procedures adopted to assess the suitability of crypto-assets in accordance with Article 76(2) of Regulation (EU) 2023/1114;
- (g) the systems, procedures and arrangement put in place to comply with Article 76(7) points (a) to (h) of Regulation (EU) 2023/1114;
- (h) the systems, procedures and arrangements to make public any bid and ask prices, the depth of trading interests at those prices which are advertised for crypto-assets through their trading platforms and price, volume and time of transactions executed in respect of crypto-assets traded on their trading platforms;
- (i) the fee structures and a justification of how they comply with the requirements laid down in Article 76(13) of Regulation (EU) 2023/1114;
- (j) the systems, procedures and arrangement to keep data relating to all orders at the disposal of the competent authority or the mechanism to ensure that the competent authority has access to the order book and any other trading system;
- (k) with regards to the settlement of transactions:
  - (i) whether the final settlement of transactions is initiated on the distributed ledger or outside the distributed ledger;
  - (ii) the timeframe within which the final settlement of crypto-asset transactions is initiated;
  - (iii) the systems and procedures to verify the availability of funds and crypto-assets;
  - (iv) the procedures to confirm the relevant details of transactions;
  - (v) the measures foreseen to limit settlement fails;
  - (vi) the definition of the moment at which settlement is final and the moment at which final settlement is initiated following the execution of the transaction.



(l) the policies and procedures and systems to detect and prevent market abuse, including information on the communications to the competent authority of possible market abuse cases.

2. Notifying entities intending to operate a trading platform for crypto-assets shall provide to the competent authority a copy of the operating rules of the trading platform and of any policies and procedures to detect and prevent market abuse.

### *Article 8*

#### **Exchange of crypto-assets for funds or other crypto-assets**

A notifying entity intending to exchange crypto-assets for funds or other crypto-assets shall provide to the competent authority all of the following information:

- (a) a description of the commercial policy established in accordance with Article 77(1) of Regulation (EU) 2023/1114;
- (b) the methodology for determining the price of the crypto-assets that the notifying entity proposes to exchange for funds or other crypto-assets in accordance with Article 77(2) of Regulation (EU) 2023/1114, including how the volume and market volatility of crypto-assets impact the pricing mechanism.

### *Article 9*

#### **Execution policy**

A notifying entity intending to provide the service of executing orders for crypto-assets on behalf of clients shall provide to the competent authority its execution policy, including all of the following:

- (a) the arrangements to ensure the client has provided consent on the execution policy prior to the execution of the order;
- (b) a list of the trading platforms for crypto-assets on which the notifying entity will rely for the execution of orders and the criteria for the assessment of execution venues included in the execution policy in accordance with Article 78(6) of Regulation (EU) 2023/1114;
- (c) which trading platforms it intends to use for each type of crypto-assets and confirmation that it will not receive any form of remuneration, discount or non-monetary benefit in return for routing orders received to a particular trading platform for crypto-assets;

- (d) how the execution factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-assets or any other relevant factors are considered as part of all necessary steps to obtain the best possible result for the client;
- (e) where applicable, the arrangements for informing clients that the notifying entity will execute orders outside a trading platform and how the notifying entity will obtain the prior express client consent before executing such orders;
- (f) how the client is warned that any specific instructions from a client may prevent the notifying entity from taking the steps that it has designed and implemented in its execution policy to obtain the best possible result for the execution of those orders in respect of the elements covered by those instructions;
- (g) the selection process for trading venues, execution strategies employed, the procedures and processes used to analyse the quality of execution obtained and how the notifying entity monitors and verifies that the best possible results were obtained for clients;
- (h) the arrangements to prevent the misuse of any information relating to clients' orders by the employees of the notifying entity;
- (i) the arrangements and procedures for how the notifying entity will disclose to clients information on its order execution policy and notify them of any material changes to their order execution policy;
- (j) the arrangements to demonstrate compliance with Article 78 of Regulation (EU) 2023/1114 to the competent authority, upon the request of the authority.

#### *Article 10*

#### **Provision of advice or portfolio management on crypto-assets**

A notifying entity intending to provide advice on crypto-assets or portfolio management of crypto-assets shall provide to the competent authority all of the following information:

- (a) the policies and procedures and a detailed description of the arrangements put in place by the notifying entity to ensure compliance with Article 81(7) of Regulation (EU) 2023/1114. This information shall include details on:
  - (i) the mechanisms to control, assess and maintain effectively the knowledge and competence of the natural persons providing advice or portfolio management on crypto-assets;
  - (ii) the arrangements to ensure that natural persons involved in the provision of advice or portfolio management are aware of, understand and apply the notifying entity's

internal policies and procedures designed to ensure compliance with Regulation (EU) 2023/1114, especially Article 81(1) of Regulation (EU) 2023/1114 and anti-money laundering and anti-terrorist financing obligations in accordance with Directive (EU) 2015/849;

- (iii) the amount of human and financial resources planned to be devoted on a yearly basis by the notifying entity to the professional development and training of the staff providing advice or portfolio management on crypto-assets;
- (b) the arrangements adopted by the notifying entity to ensure that the natural persons giving advice on behalf of the notifying entity have the necessary knowledge and expertise to conduct the suitability assessment referred to in Article 81(1) of Regulation (EU) 2023/1114.

#### *Article 11*

#### **Transfer services**

A notifying entity intending to provide transfer services for crypto-assets on behalf of clients shall provide to the competent authority all of the following information:

- (a) details on the types of crypto-assets for which the notifying entity intends to provide transfer services;
- (b) the policies and procedures and a detailed description of the arrangements put in place by the notifying entity to ensure compliance with Article 82 of Regulation (EU) 2023/1114, including detailed information on the notifying entity's arrangements and deployed ICT and human resources to address risks promptly, efficiently and thoroughly during the provision of transfer services for crypto-assets on behalf of clients, considering potential operational failures and cybersecurity risks;
- (c) if any, a description of the notifying entity's insurance policy, including on the insurance's coverage of detriment to client's crypto-assets that may result from cyber security risks;
- (d) arrangements to ensure that clients are adequately informed about the policies and procedures and arrangements referred to in point (b).

*Article 12*

**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]*

## 6.4 Annex IV – Draft ITS pursuant to Article 60(14) 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 standard forms, templates and procedures for the information to be included in the notification of certain entities of their intention to provide 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 the 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 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>16</sup>, and in particular Article 60 (14), third subparagraph, thereof,

Whereas:

- (1) It is appropriate to set out common standard forms, templates and procedures to ensure a uniform mechanism by which Member States' competent authorities effectively exercise their powers in respect of the notifications from already regulated entities that notify the relevant competent authority of their intention to become crypto-asset service providers.
- (2) The information submitted by the notifying entity should be true, accurate, complete and not misleading. In accordance with Article 60(9) of Regulation (EU) 2023/1114, where the notifying entity had previously submitted information referred to in Delegated Regulation (EU) XXXX/XXXX of [date – Regulatory Technical Standards on information to be included on notification] to the competent authority and such information is still up to date, the notifying entity should expressly indicate which information was already submitted and is still up to date.
- (3) To allow the competent authority to assess whether changes to the information provided in the notification may render the notification as not complete, it is appropriate to require notifying entities to communicate such changes without undue delay.

---

<sup>16</sup> OJ L 150, 9.6.2023, p. 40-205.

- (4) To facilitate communication between a notifying entity and the relevant competent authority, competent authorities should designate a designated contact point for the notification process and should publish the contact information on their website.
- (5) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA'), in close cooperation with the European Banking Authority.
- (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>17</sup>,

HAS ADOPTED THIS REGULATION:

*Article 1*

**Designation of a contact point**

Competent authorities shall designate a contact point for handling all information notified pursuant to Article 60 of Regulation (EU) 2023/1114. Competent authorities shall keep the contact details of the designated contact point up-to-date and shall make those contact details public on their websites.

*Article 2*

**Submission of the notification**

1. A notifying entity shall submit to the competent authority its notification by filling in the form set out in the Annex.
2. The notification shall be provided in a manner which enables storage of information in a way accessible for future reference and which allows the unchanged reproduction of the information stored.

---

<sup>17</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 3*

**Receipt of the notification and acknowledgement of receipt**

Within five working days from the receipt of the notification, the competent authority shall send electronically, on paper, or in both forms, an acknowledgement of receipt in writing to the notifying entity. That acknowledgement of receipt shall include the contact details of the department, function or staff member of the competent authority handling the notification.

*Article 4*

**Notification of changes**

The notifying entity shall notify the competent authority of any changes to the information provided in the notification and that could affect the assessment of such application without undue delay. The notifying entity shall provide the updated information by using the form set out in the Annex.

*Article 5*

**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*

*On behalf of the President*

*[Position]*



**ANNEX**

**Form for the notification of information to be provided by certain financial entities pursuant to Article 60 Regulation (EU) 2023/1114**

Date:

FROM:

Name of the notifying entity:

National reference number:

Address:

(Contact details of designated contact person):

Name:

Telephone:

Email:

TO:

Member State (if applicable):

Competent Authority:

Address:

(Contact details of the designated contact point):

Name:

Telephone:

Email:

Dear [*insert appropriate name*],

In accordance with Commission Implementing Regulation (EU) XXXX/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 standard forms, templates and procedures for the notification of certain entities of their intention to provide crypto-asset services, kindly find attached our notification of our intention to provide crypto-asset services.

We [notifying entity] declare that the submitted information is true, accurate, complete and not misleading. Unless specifically stipulated otherwise, the information is up to date on the date of this notification.

Information indicating a future date is explicitly identified in the notification and we undertake to notify the authority in writing without delay if any such information should turn out to be untrue, inaccurate, incomplete or is misleading.

- Person in charge of preparing the notification:

Name:

Status/position:

Telephone:

Email:

REQUIRED INFORMATION

*Programme of operations*

.....  
.....

Please insert the information referred to under Article 1 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Business continuity*

.....  
.....

Please insert the information referred to under Article 2 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Detection and prevention of money laundering and terrorist financing*

.....  
.....

Please insert the information referred to under Article 3 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*ICT systems and related security arrangements*

.....  
.....

Please insert the information referred to under Article 4 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Segregation of clients' crypto-assets and funds*

.....  
.....

Please insert the information referred to under Article 5 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Custody and administration policy*

.....  
.....

Please insert the information referred to under Article 6 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Operating rules of the trading platform and market abuse detection*

.....  
.....

Please insert the information referred to under Article 7 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Exchange of crypto-assets for funds or other crypto-assets*

.....  
.....

Please insert the information referred to under Article 8 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Execution policy*

.....  
.....

Please insert the information referred to under Article 9 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Provision of advice or portfolio management on crypto-assets*

.....  
.....

Please insert the information referred to under Article 10 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification.

*Transfer services*

.....  
.....

Please insert the information referred to under Article 11 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on notification for CASPs], by setting out that information here or making reference to the relevant sections of the notification

Yours sincerely,

[signature]



## 6.5 Annex V – Draft RTS pursuant to Article 62(5) 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 information to be included in an application for authorisation as crypto-asset service provider**

(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 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>18</sup>, and in particular Article 62(5), third subparagraph, thereof,

Whereas:

- (1) The information to be provided in an application for authorisation as crypto-asset service provider should be sufficiently detailed and comprehensive to enable competent authorities to assess whether an applicant meets the applicable requirements laid down in Title V and, where relevant, Title VI of Regulation (EU) 2023/1114.
- (2) The competent authority should retain the right to request additional information from the applicant during the assessment process in accordance with the criteria and timelines set out in Regulation (EU) 2023/1114.
- (3) The application for authorisation as crypto-asset service provider should contain personal data about the identity of the applicant seeking authorisation as a crypto-asset service provider, the governance arrangements and internal control mechanisms, the suitability of the members of the management body and the sufficiently good repute of the shareholders or members with qualifying holdings. 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 applicant issuer, of its ability to comply with the relevant requirements of Regulation (EU) 2023/1114, and that it does not fall into any ground of refusal of the authorisation set out in points (a) to (d) of Article 63(10) of that Regulation. When assessing the application and processing the personal data included therein, competent authorities should comply with the relevant provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>19</sup>, and the ECB, ESMA and the EBA should comply with Regulation (EU) 2018/1725.

---

<sup>18</sup> OJ L 150, 9.6.2023, p. 40-205.

<sup>19</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).

- (4) To ensure that the competent authority's assessment is based on accurate information, it is essential that an applicant provides copies of its corporate documents, including its legal entity identifier, the articles of association, a copy of registration of the applicant in the national register of companies and, where the applicant intends to operate a trading platform, the commercial name used.
- (5) An application for authorisation as crypto-asset service provider should contain a programme of operations, describing the applicant's organisational structure, strategy in providing crypto-asset services to its targeted clients and its operational capacity for the three years following authorisation. Where describing the strategy used to target clients, the applicant should describe the marketing means that it intends to use such as, for instance, websites, mobile phone applications, face-to-face meetings, press releases, or any form of physical or electronic means, including social media campaign tools, internet advertisements or banners, retargeting of advertising, agreements with influencers, sponsorships agreements, calls, webinars, any invitation to an event, affiliation campaign, gamification techniques, invitation to fill in a response form or to follow a training course, demo accounts or educational materials.
- (6) The competent authority should be able to assess the applicant's resilience to withstand external financial shocks, including those concerning the value of crypto-assets. Therefore, the applicant should include stress scenarios simulating severe but plausible events in its forecast calculations and plans to determine its own funds.
- (7) Clients are exposed to potential risks related to the crypto-asset service providers. In order to enable competent authorities to assess whether applicants meet the requirements set out in Article 67 Regulation (EU) 2023/1114 to protect clients against such risks, an application should contain an obligatory set of information describing the applicant's prudential safeguards.
- (8) To ensure that crypto-asset service providers comply with their obligations in accordance with Regulation (EU) 2023/1114, applicants should demonstrate that they have adequate and robust governance arrangements and internal control mechanisms, as such arrangements and mechanisms are essential to the sound and prudent management of crypto-asset service providers.
- (9) In the financial services system, time is often of the essence. It is thus critical to maintain operations or at least essential functions and to minimise downtime due to unexpected disruptions (such as cyberattacks, natural disasters) to avoid outages as they can have major financial, regulatory and reputational consequences for the crypto-asset service provider and crypto-assets markets more generally. An application should thus contain detailed information on the applicant's arrangements to ensure continuity and regularity in the performance of its crypto-asset services, including a detailed description of its business continuity and disaster recovery plans.
- (10) Effective mechanisms, systems and policies and procedures in compliance with Directive (EU) 2015/849 of the European Parliament and of the Council<sup>20</sup> are crucial to ensure that applicants appropriately address risks and practices of money laundering and terrorist

---

<sup>20</sup> Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

financing in the provision of crypto-asset services. Thus, applicants should provide detailed information on their mechanisms, systems and policies and procedures on how they prevent, inter alia, anti-money laundering and counter-terrorist financing risks associated with their business activities.

- (11) As one of the requirements to ensure that the crypto-asset service provider will act fairly and honestly, it is necessary that applicants provide the information and documents to prove that the members of the management body are of sufficiently good repute and have sufficient knowledge, skills and experience. Notably, the applicant should provide the competent authorities with all information about past criminal convictions and with information on pending criminal investigations, civil and administrative cases, penalties, enforcement actions and other adjudicatory proceedings of the members of the management body relating to commercial law, insolvency law, anti-money laundering, counter-terrorist financing, fraud, professional liability. In order to provide competent authorities with adequate information on the reputation of the members of the management body, the information should be provided for those cases directly concerning the member or concerning an organisation of which the member held a position as member of the management body, shareholder or member with qualifying holdings or a key function holder. To ensure that competent authorities receive sufficient information on refusals or withdrawals of, inter alia, registrations, authorisations or memberships related to the applicant's provision of crypto-asset services, the applicant should provide such information about any member of the management body. Additionally, applicants should provide, for each member of the management body, relevant information to enable competent authorities to assess their professional experience, knowledge and skills in the scope of the position sought and a description of all financial and non-financial interests of the members of the management body that could create potential material conflicts of interest significantly affecting the members' perceived trustworthiness in the performance of their mandate.
- (12) In respect of the requirement of good repute of shareholders and members directly or indirectly holding qualifying holdings in the applicant, the application should contain all information about past convictions and pending criminal investigations, civil and administrative cases and other adjudicatory proceedings as well as relevant information relating to the certainty and legitimate origin of the funds used to set-up the applicant and finance its business so to enable the assessment of any attempt or suspicion of money laundering or terrorist financing.
- (13) Due to the decentralised and digital nature of crypto-assets, cybersecurity risks for crypto-asset service providers are significant and take many forms. To ensure that applicants are able to prevent data breaches and financial losses that may be caused by cyberattacks, competent authorities should be provided with information on the applicants' deployed ICT systems and related security arrangements, including the human resources dedicated to addressing cybersecurity risks.
- (14) The segregation of client crypto-assets and funds is an important part of the regime regulating crypto-asset services as it protects clients from losses of the crypto-asset service provider and from misuse of their crypto-assets and funds. Crypto-asset service providers are therefore subject to an obligation to make adequate arrangements to safeguard clients' ownership rights. This requirement also applies to crypto-asset service providers which do not provide custody and administration services.

- (15) To allow national competent authorities to assess the adequacy of the applicant's operating rules of trading platforms for crypto-assets, specific elements should be detailed in their description. In particular, the applicant should elaborate aspects of the operating rules relating to the admission to trading of crypto-assets, the trading and the settlement of crypto-assets. Relating to the admission to trading, applicants should provide detailed information on rules governing the admission of crypto-assets to trading, the way in which the admitted crypto-assets comply with the applicant's rules, the types of crypto-assets that the applicant will not admit to its platform and the reasons for these exclusions and fees applicable to the admission to trading. As for the trading of crypto-assets, the applicant should further specify in the description of the operating rules, the elements of those rules which govern the execution and cancelation of orders, elements which aim at ensuring orderly trading and transparency and record-keeping rules. Finally, the applicant should include in the description of the operating rules the elements governing the settlement of transactions of crypto-assets concluded on the trading platform, including whether the settlement of transactions is initiated in the Distributed Ledger Technology (DLT), the timeframe in which the execution is initiated, the definition of the moment at which the settlement is final, all verifications required to ensure the effective settlement of the transaction and any measure in place to limit settlement failures.
- (16) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority (ESMA) to the European Commission, as developed in close cooperation with the European Banking Authority (EBA).
- (17) 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>21</sup>,

HAS ADOPTED THIS REGULATION:

### *Article 1*

#### **General information**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority an application that includes all of the following information:

- (a) the legal name, phone number and email of the applicant;

---

<sup>21</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).

- (b) any commercial or trading name used or to be used by the applicant;
- (c) the legal entity identifier (LEI) of the applicant;
- (d) the full name, function, email address and telephone number of the designated contact point or person;
- (e) the legal form of the applicant (including information on whether it will be a legal person or other undertaking) and, where available, its national identification number as well as evidence of its registration with the national register of companies;
- (f) date and Member State of the applicant's incorporation or foundation;
- (g) where applicable, the instruments of constitution, the articles of association and by-laws;
- (h) the address of the head office and, if different, of the registered office of the applicant;
- (i) information on where the branches will operate, if any, and their legal entity identifiers (LEI), if available;
- (j) the domain name of each website operated by the applicant and the social media accounts of that applicant;
- (k) where the applicant is not a legal person, documentation to assess whether the level of protection ensured to third parties interests and the rights of the holders of crypto-assets, including in case of insolvency, is equivalent to that afforded by legal persons and that the applicant is subject to equivalent prudential supervision appropriate to their legal form,
- (l) where the applicant intends to operate a trading platform for crypto-assets:
  - (i) the physical address, phone number and email of the trading platform for crypto-assets;
  - (ii) any commercial name of the trading platform for crypto-assets.

## *Article 2*

### **Programme of operations**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority the programme of operations for the following three years, including all of the following information:

- (a) where the applicant belongs to a group, an explanation of how the activities of the applicant will fit within the group strategy and interact with the activities of the other entities of the

group, including an overview of the current and planned organisation and structure of the group;

- (b) an explanation of how the activities of the entities affiliated with the applicant, including where there are regulated entities in the group, is expected to impact the activities of the applicant. This explanation shall include a list of and information on the entities affiliated with the applicant, including where there are regulated entities, the services provided by these entities (including regulated services, activities and types of clients) and the domain names of each website operated by such entities;
- (c) a list of crypto-asset services that the applicant intends to provide as well as the types of crypto-assets to which the crypto-asset services will relate;
- (d) other planned activities, regulated in accordance with Union or national law or unregulated, including any services, other than crypto-asset services, that the applicant intends to provide;
- (e) whether the applicant intends to offer crypto-assets to the public or seek admission to trading of crypto-assets and if so, of what type of crypto-assets;
- (f) a list of jurisdictions, in and outside the European Union, in which the applicant plans to provide crypto-asset services, including information on the domicile of targeted clients and the targeted number by geographical area;
- (g) types of prospective clients targeted by the applicant's services;
- (h) a description of the means of access to the applicant's crypto-asset services by clients, including all of the following :
  - (i) the domain names for each website or other ICT-based application through which the crypto-asset services will be provided by the applicant and information on the languages in which the website will be available, the types of crypto-asset services that will be accessed through it and, where applicable, from which Member States the website will be accessible;
  - (ii) the name of any ICT-based application available to clients to access the crypto-asset services, in which languages it is available and which crypto-asset services can be accessed through it;
- (i) the planned marketing and promotional activities and arrangements for the crypto-asset services, including:



- (i) all means of marketing to be used for each of the services, the means of identification that the applicant intends to use and information on the relevant category of clients targeted and types of crypto-assets;
- (ii) languages that will be used for the marketing and promotional activities;
- (j) a detailed description of the human, financial and ICT resources allocated to the intended crypto-asset services as well as their geographical location;
- (k) the applicant's outsourcing policy and a detailed description of the applicant's planned outsourcing arrangements, including intra-group arrangements, how the applicant intends to comply with the requirements set out in Article 73 of Regulation (EU) 2023/1114. The applicant shall also include information on the functions or person responsible for outsourcing, the resources (human and ICT) allocated to the control of the outsourced functions, services or activities of the related arrangements and on the risk assessment related to the outsourcing;
- (l) the list of entities that will provide outsourced services, their geographical location and the relevant services outsourced;
- (m) a forecast accounting plan including stress scenarios at an individual and, where applicable, at consolidated group and sub-consolidated level in accordance with Directive 2013/34/EU. The financial forecast shall consider any intra-group loans granted or to be granted by and to the applicant;
- (n) any exchange of crypto-assets for funds and other crypto-asset activities that the applicant intends to undertake, including through any decentralised finance applications with which the applicant wishes to interact on its own account.

2. Where the applicant intends to provide the service of reception and transmission of orders for crypto-assets on behalf of clients, it shall provide to the competent authority a copy of the policies and procedures and a description of the arrangements ensuring compliance with the requirements set out in Article 80 of Regulation (EU) 2023/1114.

3. Where the applicant intends to provide the service of placing of crypto-assets, it shall provide to the competent authority a copy of the policies and procedures and a description of the arrangements in place to comply with Article 79 of Regulation (EU) 2023/1114 as well as Article 9 of [RTS on conflicts of interest of CASPs].



### *Article 3*

#### **Prudential requirements**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority all of the following information:

- (a) a description of the applicant's prudential safeguards in accordance with Article 67 of Regulation (EU) 2023/1114, consisting of:
  - (i) the amount of the prudential safeguards that the applicant has in place at the time of the application for authorisation and the description of the assumptions used for its determination;
  - (ii) the amount of the prudential safeguards covered by own funds referred to in Article 67(4), point (a), of Regulation (EU) 2023/1114, where applicable;
  - (iii) the amount of the applicant's prudential safeguards covered by an insurance policy referred to in Article 67(4), point (b), of Regulation (EU) 2023/1114, where applicable;
- (b) forecast calculations and plans to determine own funds, including:
  - (i) forecast calculation of the applicant's prudential safeguards for the first three business years;
  - (ii) planning assumptions including stress scenarios for the above forecast as well as explanations of the figures;
  - (iii) expected number and type of clients, volume of orders and transactions and expected maximum amount of crypto-assets under custody;
- (c) for companies that are already active, the financial statements of the last three years approved, where audited, by the external auditor;
- (d) a description of the applicant's prudential safeguards planning and monitoring policies and procedures;
- (e) proof that the applicant meets the prudential safeguards in accordance with Article 67 of Regulation (EU) 2023/1114, including:
  - (i) in relation to own funds:
    - documentation on how the applicant has calculated the amount in accordance with Article 67 of Regulation (EU) 2023/1114;

- for companies that are already active and whose financial statements are not audited, a certification by the national supervisor of the amount of own funds of the applicant;
  - for undertakings in the process of being incorporated, a statement issued by a bank certifying that the funds are deposited in the applicant's bank account;
- (ii) in relation to the insurance policy or comparable guarantee:
- the legal name, the date and Member State of incorporation or foundation, the address of the head office and, if different, of the registered office and contact details of the undertaking authorised to provide the insurance policy or comparable guarantee;
  - a copy of the subscribed insurance policy incorporating all the elements necessary to comply with Article 67(5) and (6) of Regulation (EU) 2023/1114, where available, or
  - a copy of the insurance agreement incorporating all the elements necessary to comply with Article 67(5) and (6) of Regulation (EU) 2023/1114 signed by an undertaking authorised to provide insurance in accordance with Union law or national law.

#### *Article 4*

##### **Information about governance arrangements and internal control mechanisms**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority the following information on its governance arrangements and internal control mechanisms:

- (a) a detailed description of the organisational structure of the applicant, where relevant encompassing the group, including the indication of the distribution of the tasks and powers and the relevant reporting lines and the internal control arrangements implemented together with an organisational chart;
- (b) the personal details of the heads of internal functions (management, supervisory and internal control functions), including their location and a curriculum vitae, stating relevant education, and professional training and professional experience and a description of the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them;

- (c) the policies and procedures and a detailed description of the arrangements put in place to ensure that relevant staff are aware of the policies and procedures which must be followed for the proper discharge of their responsibilities;
- (d) the policies and procedures and a detailed description of the arrangements put in place to maintain adequate and orderly records of the business and internal organisation of the applicant in accordance with Article 68(9) of Regulation (EU) 2023/1114;
- (e) the policies and procedures and arrangements to enable the management body to assess and periodically review the effectiveness of the policy arrangements and procedures put in place to comply with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114 in accordance with Article 68(6) of the same Regulation including all of the following:
  - (i) identification of the internal control functions in charge of monitoring the policy arrangements and procedures put in place to comply with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114, together with the scope of their responsibility and reporting lines to the management body of the applicant;
  - (ii) indication of the periodicity of internal control functions reporting to the management body of the applicant on the effectiveness of the policy arrangements and procedures put in place to comply with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114;
  - (iii) explanation of how the applicant ensures that the internal control functions operate independently and separately from the functions they control, have access to the necessary resources and information, and that those internal control functions can report directly to the management body of the applicant both at least once a year and on an ad hoc basis including where they detect a significant risk of failure for the applicant to comply with its obligations;
  - (iv) a description of the ICT systems, safeguards and controls put in place to monitor the activities of the applicant and ensure compliance with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114, including back-up systems, and ICT systems and risk controls, where not provided in accordance with Article 9 of this Regulation;
- (b) the policies and procedures and a detailed description of the arrangements established by the applicant to ensure compliance with its obligations under Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114, including;
  - (i) the applicant's record keeping arrangements in accordance with [*RTS on record-keeping by crypto-asset services providers*];
  - (ii) a detailed description of the procedures for the applicant's employees to report potential or actual infringements of Regulation (EU) 2023/1114 in accordance with Article 116 of Regulation (EU) 2023/1114;

- (c) where relevant, a description of the arrangements put in place to prevent and detect market abuse in accordance with Article 92 of Regulation (EU) 2023/1114;
- (d) whether the applicant has appointed or will appoint external auditors and, if that is the case, their name and contact details, when available;
- (e) the accounting policies and procedures by which the applicant will record and report its financial information, including the start and end dates of the applied accounting year.

2. As part of the information on policies and procedures established to ensure compliance with Chapters 2 and 3 of Title V of Regulation (EU) 2023/1114, applicants shall provide to the competent authority all of the following information on the management of risks relating to conflicts of interests:

- (a) a copy of the applicant's conflicts of interest policy, together with a description of how the policy:
  - (i) ensures that the applicant identifies and prevents or manages conflicts of interests in accordance with Article 72(1) of Regulation (EU) 2023/1114 and discloses conflicts of interest in accordance with Article 72(2) of Regulation (EU) 2023/1114;
  - (ii) is commensurate to the scale, nature and range of crypto-asset services that the applicant intends to provide and of the other activities of the group to which it belongs;
  - (iii) ensures that the remuneration policies and procedures and arrangements do not create conflicts of interest;
- (b) how the applicant's conflicts of interest policy ensures compliance with Article 4(9) of [*RTS on conflicts of interest of CASPs*], including information on the systems and arrangements put in place by the applicant to:
  - (i) monitor, assess, review the effectiveness of its conflicts of interests policy and remedy any deficiencies;
  - (ii) record cases of conflicts of interests, including the identification, assessment, remedy and whether the case was disclosed to the client.

#### *Article 5*

### **Business continuity**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall submit to the competent authority a detailed

description of the applicant's business continuity plan, including which steps shall be taken to ensure continuity and regularity in the performance of the applicant's crypto-asset services.

2. The description shall include details showing that the established business continuity plan is appropriate and that arrangements are set up to maintain and periodically test it. The description shall explain, with regard to critical or important functions supported by third-party service providers, how business continuity is ensured in the event that the quality of the provision of such functions deteriorates to an unacceptable level or fails. The description shall also explain how business continuity is ensured in the event of the death of a key person and, where relevant, political risks in the service provider's jurisdiction.

### *Article 6*

#### **Detection and prevention of money laundering and terrorist financing**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide the competent authority with information on its internal control mechanisms and policies and procedures to ensure compliance with the provisions of national law transposing Directive (EU) 2015/849 and with information on the risk assessment framework to manage risks relating to money laundering and terrorist financing, including all of the following:

- (a) the applicant's assessment of the inherent and residual risks of money laundering and terrorist financing associated with its business, including the risks relating to the applicant's customer base, to the services provided, to the distribution channels used and to the geographical areas of operation;
- (b) the measures that the applicant has or will put in place to prevent the identified risks and comply with applicable anti-money laundering and counter-terrorist financing requirements, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;
- (c) detailed information on how such mechanisms, systems and procedures are adequate and proportionate to the scale, nature, inherent money laundering and terrorist financing risk, range of crypto-asset services provided, the complexity of the business model and how they ensure the applicant's compliance with Directive (EU) 2015/849 and Regulation (EU) 2023/1113;
- (d) the identity of the person in charge of ensuring the applicant's compliance with anti-money laundering and counter-terrorist financing obligations, and evidence of the person's skills and expertise;

- (e) arrangements, human and financial resources devoted to ensure that staff of the applicant is appropriately trained in anti-money laundering and counter-terrorist financing matters (annual indications) and on specific crypto-asset related risks;
- (f) a copy of the applicant's anti-money laundering and counter-terrorism policies and procedures, and systems;
- (g) the frequency of the assessment of the adequacy and effectiveness of such mechanisms, systems and policies and procedures as well as the person or function responsible for such assessment.

#### *Article 7*

#### **Identity and proof of good repute, knowledge, skills, experience and of sufficient time commitment of the members of the management body**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide the competent authority with all of the following information for each member of the management body:

- (a) the full name and, where different, name at birth;
- (b) the place and date of birth, address and contact details of the current place of residence and of any other place of residence in the past ten years, nationalit(y/ies), personal national identification number and copy of an official identity document or equivalent;
- (c) details of the position held or to be held by the person, including whether the position is executive or non-executive, the start date or planned start date and, where applicable, the duration of mandate, and a description of the person's key duties and responsibilities;
- (d) a curriculum vitae stating relevant education, professional training and professional experience with the name and nature of all organisations for which the individual has worked and the nature and duration of the functions performed, in particular highlighting any activities within the scope of the position sought, including professional experience relevant to financial services, crypto-assets, or other digital assets, distributed ledger technology, information technology, cybersecurity, or digital innovation; for positions held in the previous 10 years. When describing the aforementioned activities, details shall be included on all delegated powers and internal decision-making powers held and the areas of operations under control;
- (e) documentation relating to the person's reputation and experience, in particular a list of reference persons including contact information and letters of recommendation;
- (f) personal history, including all of the following:

- (i) criminal records, including criminal convictions and any ancillary penalties and information on pending criminal proceedings or investigations or penalties (including relating to commercial law, financial services law, money laundering, and terrorist financing, fraud or professional liability), information on enforcement proceedings or sanctions, information on relevant civil and administrative cases and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, through an official certificate (if and so far as it is available from the relevant Member State or third country), or through another equivalent document or, where such certificate does not exist. For ongoing investigations, the information may be provided through a declaration of honour. Official records, certificates and documents shall have been issued within three months before the submission of application for an authorisation;
  - (ii) information on any refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; or the withdrawal, revocation or termination of such a registration, authorisation, membership or licence to carry out a trade, business or profession; or any expulsion by a regulatory or government body or by a professional body or association;
  - (iii) information on dismissal from employment or a position of trust, fiduciary relationship, or similar situation;
  - (iv) information on whether another competent authority has assessed the reputation of the individual, including the identity of that authority, the date of the assessment and information about the outcome of that assessment. The applicant shall not need to submit such information about the previous assessment where the competent authority is already in possession of such information;
- (g) a description of any financial and non-financial interests or relationships of the person and his/her close relatives to members of the management body and key function holders in the same institution, the parent institution and subsidiaries and shareholders. Such description shall include any financial interests, including crypto-assets, other digital assets, loans, shareholdings, guarantees or security interests, whether granted or received, commercial relationships, legal proceedings and whether the person was a politically exposed person as defined in point (9) of article 3 of Directive (EU) 2015/849 over the past two years.
- (h) where a material conflict of interest is identified, a statement of how that conflict will be satisfactorily mitigated or remedied, including a reference to the outline of the conflicts of interest policy;
- (i) information on the time that will be devoted to the performance of the person's functions within the applicant, including all of the following:



- (i) the estimated minimum time, per year and per month, that the individual will devote to the performance of his or her functions within the applicant;
- (ii) a list of the other executive and non-executive directorships that the person holds, referring to commercial and non-commercial activities or set up for the sole purposes of managing the economic interests of the person concerned;
- (iii) information on the size and complexity of the companies or organisations where the mandates referred to in point (ii) are held, including total assets, based on the last available annual accounts whether or not the company is listed and the number of employees of those companies or organisations;
- (iv) a list of any additional responsibilities associated with the mandates referred to in point (ii), including chairing a committee;
- (v) the estimated time in days per year dedicated to each of the other mandates referred to in point (ii) and the number of meetings per year dedicated to each mandate.

2. For the purposes of paragraph 1, points (f)(i) and (ii), the applicant shall provide the information through an official certificate (if and so far as it is available from the relevant Member State or third country), or through another equivalent document, where such certificate does not exist. Official records, certificates and documents shall have been issued within three months before the submission of application for an authorisation. For ongoing investigations, the information may be provided through a declaration of honour.

3. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide the competent authority with the suitability policy and the results of any suitability assessment of each member of the management body performed by the applicant, and the results of the assessment of the collective suitability of the management body, including the relevant board minutes or suitability assessment report or documents on the outcome of the suitability assessment.

### *Article 8*

#### **Information relating to shareholders or members with qualifying holdings**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide the competent authority with all of the following information:

- (a) a detailed organigram of the holding structure of the applicant, including the breakdown of its capital and voting rights and the names of the shareholders or members with qualifying holdings;

- (b) for each shareholder or member holding a direct or indirect qualifying holding in the applicant, the information and documents set out in Articles 1 to 4 of the [*RTS specifying the content of the information necessary to carry out the assessment of the proposed acquisition of a qualifying holding*] as applicable;
- (c) the identity of each member of the management body who will direct the business of the applicant and will have been appointed by, or following a nomination from, such shareholder or member with qualifying holdings;
- (d) for each shareholder or member holding a direct or indirect qualifying holding, information on the number and type of shares or other holdings subscribed, their nominal value, any premium paid or to be paid, any security interests or encumbrances, including the identity of the secured parties.
- (e) information referred to in Article 6, points (b), (d) and (e) and in Article 8 of the [*RTS specifying the content of the information necessary to carry out the assessment of the proposed acquisition of a qualifying holding*].

#### *Article 9*

#### **ICT systems and related security arrangements**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority all of the following information:

- (a) technical documentation of the ICT systems, on DLT infrastructure relied upon, where relevant, and on the security arrangements. The applicant shall include a description of the arrangements and deployed ICT and human resources established to ensure that the applicant complies with Regulation (EU) 2022/2554, including, but not limited to:
  - (i) a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system, including a detailed description of ICT systems, protocols and tools and of how the applicant's procedures, policies and systems to safeguard the security, integrity, availability, authenticity and confidentiality of data in accordance with Regulation (EU) 2022/2554 and Regulation (EU) 2016/679;
  - (ii) an identification of ICT services supporting critical or important functions, developed or maintained by the applicant, as well as those provided by third-party service providers, a description of such contractual arrangements (identity and geographical location of the providers, description of the outsourced activities or ICT services with their main characteristics, copy of contractual agreements) and how they comply with

Article 73 of Regulation (EU) 2023/1114 and the Chapter V of Regulation (EU) 2022/2554;

- (iii) a description of the applicant's procedures, policies, arrangements and systems for security and incident management;
- (b) a cybersecurity audit realized by a third-party cybersecurity auditor having sufficient experience in accordance with [DORA TLPT RTS detailing the minimum requirements on capabilities which are described in DORA Level 1 Article 27] covering: the following audits or tests performed by external independent parties:
  - (i) organisational cybersecurity, physical security and secure software development lifecycle arrangements;
  - (ii) vulnerability assessments and scans, network security assessments;
  - (iii) configuration reviews of ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554;
  - (iv) penetration tests on the ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554, in accordance with all the following audit test approaches:
    - black box: the auditor has no information other than the IP addresses and URLs associated with the audited target. This phase is generally preceded by the discovery of information and the identification of the target by querying domain name system (DNS) services, scanning open ports, discovering the presence of filtering equipment, etc.;
    - grey box phase: auditors have the knowledge of a standard user of the information system (legitimate authentication, "standard" workstation, etc.). The identifiers can belong to different user profiles in order to test different privilege levels;
    - white box phase: auditors have as much technical information as possible (architecture, source code, telephone contacts, identifiers, etc.) before starting the analysis. They also have access to technical contacts related to the target.
  - (v) if the applicant uses and/or develops smart-contracts, a cybersecurity source code review of them.
- (c) a description of conducted audits of the ICT systems including used DLT infrastructure and security arrangements;

- (d) a description of the relevant information set out in subparagraphs a) and b) in non-technical language of the information provided under points a) and b).

#### *Article 10*

### **Segregation of clients' crypto-assets and funds**

1. Where the applicant intends to hold crypto-assets belonging to clients or the means of access to such crypto-assets, or clients' funds (other than e-money tokens), the applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority a detailed description of its policies and procedures for the segregation of clients' crypto-assets and funds, including all of the following:

- (a) how the applicant ensures that
- (i) clients' funds are not used for its own account;
  - (ii) crypto-assets belonging to the clients are not used for its own account;
  - (iii) the wallets holding clients' crypto-assets are different from the applicant's own wallets;
- (b) a detailed description of the approval system for cryptographic keys and safeguarding of cryptographic keys (for instance, multi-signature wallets);
- (c) how the applicant segregates clients' crypto-assets, including from other clients' crypto-assets in the event of wallets containing crypto-assets of more than one client (omnibus accounts);
- (d) a description of the procedure to ensure that clients' funds (other than e-money tokens) are deposited with a central bank or a credit institution by the end of the business day following the day on which they were received and are held in an account separately identifiable from any accounts used to hold funds belonging to the applicant;
- (e) where the applicant does not intend to deposit funds with the relevant central bank, which factors the applicant is taking into account to select the credit institutions to deposit clients' funds, including the applicant's diversification policy, where available, and the frequency of review of the selection of credit institutions to deposit clients' funds;
- (f) how the applicant ensures that clients are informed in clear, concise and non-technical language about the key aspects of the applicant's systems and policies and procedures to comply with Article 70(1), (2) and (3) of Regulation (EU) 2023/1114.

2. In accordance with Article 70(5) of Regulation (EU) 2023/1114, crypto-asset service providers that are electronic money institutions or payment institutions shall only provide the information listed in paragraph 1 above in relation to the segregation of clients' crypto-assets.

#### *Article 11*

### **Complaints-handling**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall provide to the competent authority a detailed description of the applicant's complaints handling policies and procedures, including all of the following:

- (a) information on the human and technical resources allocated to complaints handling;
- (b) information on the person in charge of the resources dedicated to the management of complaints, together with a curriculum vitae stating relevant education, professional training and professional experience justifying the skills, knowledge and expertise for the discharge of the responsibilities allocated to him or her;
- (c) how the applicant ensures compliance with the requirements set out in Article 1 of [*RTS on complaints handling by CASPs*];
- (d) how the applicant will inform clients or potential clients of the possibility to file a complaint free of charge, including where and how on the applicant's website, or on any other relevant digital device that may be used by clients to access the crypto-asset services, is the information available as well as what information is provided;
- (e) the applicant's record-keeping arrangements in relation to complaints;
- (f) the timeline provided in the complaints-handling policies and procedures of the applicant to investigate, respond and, where appropriate, take measures in response to complaints received;
- (g) how the applicant will inform clients or potential clients of the available remedies;
- (h) the procedural key steps of the applicant in making a decision on a complaint and how the applicant will communicate this decision to the client or potential client who filed the complaint.

## Article 12

### **Custody and administration policy**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to provide the service of custody and administration of crypto-assets on behalf of clients shall provide to the competent authority all of the following information:

- (a) a description of the arrangements linked to the type or types of custody offered to clients, a copy of the applicant's standard agreement for the custody and administration of crypto-assets on behalf of clients as well as a copy of the summary of the custody policy made available to clients in accordance with Article 75(3) of Regulation (EU) 2023/1114;
- (b) the applicant's custody and administration policy, including a description of identified sources of operational and ICT risks for the safekeeping and control of the crypto-assets or the means of access to the crypto-assets of clients, together with:
  - (i) the policies and procedures, and a description of, the arrangements to ensure compliance with Article 75(8) of Regulation (EU) 2023/1114;
  - (ii) the policies and procedures, and a description of the systems and controls, to manage those risks, including when the custody and administration of crypto-assets on behalf of clients is outsourced to a third party;
  - (iii) the policies and procedures relating to, and a description of, the systems to ensure the exercise of the rights attached to the crypto-assets by the clients;
  - (iv) the policies and procedures relating to, and a description of, the systems to ensure the return of crypto-assets or the means of access to the clients;
- (c) information on how the crypto-assets and the means of access to the crypto-assets of the clients are identified;
- (d) information on arrangements to minimise the risk of loss of crypto-assets or of means of access to crypto-assets;
- (e) where the crypto-asset service provider has delegated the provision of custody and administration of crypto-assets on behalf of clients to a third-party:
  - (i) information on the identity of any third-party providing the service of custody and administration of crypto-assets and its status in accordance with Article 59 or Article 60 of Regulation (EU) 2023/1114;

- (ii) a description of any functions relating to the custody and administration of crypto-assets delegated by the crypto-asset service provider, the list of any delegates and sub-delegates (as applicable) and any conflicts of interest that may arise from such a delegation.
- (iii) a description of how the applicant intends to supervise the delegations or sub-delegations.

### *Article 13*

#### **Operating rules of the trading platform and market abuse detection**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to operate a trading platform for crypto-assets shall provide to the competent authority a description of all of the following:

- (a) rules regarding the admission of crypto-assets to trading;
- (b) the approval process for admitting crypto-assets to trading, including the customer due diligence carried out in accordance with Directive (EU) 2015/849;
- (c) the list of any categories of crypto-assets that will not be admitted to trading and the description of the reasons for such exclusion;
- (d) the policies and procedures and fees for the admission to trading, together with a description, where relevant, of membership, rebates and the related conditions;
- (e) the rules governing order execution, including any cancellation procedures for executed orders and for disclosing such information to market participants;
- (f) the policies and procedures adopted to assess the suitability of crypto-assets in accordance with Article 76(2) of Regulation (EU) 2023/1114;
- (g) the systems, procedures and arrangement put in place to comply with Article 76(7) points (a) to (h) of Regulation (EU) 2023/1114;
- (h) the systems, procedures and arrangements to make public any bid and ask prices, the depth of trading interests at those prices which are advertised for crypto-assets through their trading platforms and price, volume and time of transactions executed in respect of crypto-assets traded on their trading platforms;
- (i) the fee structures and a justification of how they comply with the requirements laid down in Article 76(13) of Regulation (EU) 2023/1114;



- (j) the systems, procedures and arrangement to keep data relating to all orders at the disposal of the competent authority or the mechanism to ensure that the competent authority has access to the order book and any other trading system;
- (k) with regards to the settlement of transactions:
  - (i) whether the final settlement of transactions is initiated on the distributed ledger or outside the distributed ledger;
  - (ii) the timeframe within which the final settlement of crypto-asset transactions is initiated;
  - (iii) the systems and procedures to verify the availability of funds and crypto-assets;
  - (iv) the procedures to confirm the relevant details of transactions;
  - (v) the measures foreseen to limit settlement fails;
  - (vi) the definition of the moment at which settlement is final and the moment at which final settlement is initiated following the execution of the transaction;
- (l) the policies and procedures and systems to detect and prevent market abuse, including information on the communications to the competent authority of possible market abuse cases.

2. Applicants intending to operate a trading platform for crypto-assets shall provide to the competent authority a copy of the operating rules of the trading platform and of any policies and procedures to detect and prevent market abuse.

#### *Article 14*

### **Exchange of crypto-assets for funds or other crypto-assets**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to provide the service of exchange of crypto-assets for funds or other crypto-assets shall provide to the competent authority all of the following information:

- (a) a description of the commercial policy established in accordance with Article 77(1) of Regulation (EU) 2023/1114;
- (b) the methodology for determining the price of the crypto-assets that the applicant proposes to exchange for funds or other crypto-assets in accordance with Article 77(2) of Regulation (EU) 2023/1114, including how the volume and market volatility of crypto-assets impact the pricing mechanism.

*Article 15*

**Execution policy**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to provide the service of executing orders for crypto-assets on behalf of clients shall provide to the competent authority its execution policy, including all of the following:

- (a) the arrangements to ensure the client has provided consent on the execution policy prior to the execution of the order;
- (b) a list of the trading platforms for crypto-assets on which the applicant will rely for the execution of orders and the criteria for the assessment of execution venues included in the execution policy in accordance with Article 78(6) of Regulation (EU) 2023/1114;
- (c) which trading platforms it intends to use for each type of crypto-assets and confirmation that it will not receive any form of remuneration, discount or non-monetary benefit in return for routing orders received to a particular trading platform for crypto-assets;
- (d) how the execution factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-assets or any other relevant factors are considered as part of all necessary steps to obtain the best possible result for the client;
- (e) where applicable, the arrangements for informing clients that the applicant will execute orders outside a trading platform and how the applicant will obtain the prior express client consent before executing such orders;
- (f) how the client is warned that any specific instructions from a client may prevent the applicant from taking the steps that it has designed and implemented in its execution policy to obtain the best possible result for the execution of those orders in respect of the elements covered by those instructions;
- (g) the selection process for trading venues, execution strategies employed, the procedures and processes used to analyse the quality of execution obtained and how the applicant monitors and verifies that the best possible results were obtained for clients;
- (h) the arrangements to prevent the misuse of any information relating to clients' orders by the employees of the applicant;
- (i) the arrangements and procedures for how the applicant will disclose to clients information on its order execution policy and notify them of any material changes to their order execution policy;

- (j) the arrangements to demonstrate compliance with Article 78 of Regulation (EU) 2023/1114 to the competent authority, upon the request of the authority.

#### *Article 16*

### **Provision of advice or portfolio management on crypto-assets**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to provide advice on crypto-assets or portfolio management of crypto-assets shall provide to the competent authority all of the following information:

- (a) the policies and procedures and a detailed description of the arrangements put in place by the applicant to ensure compliance with Article 81(7) of Regulation (EU) 2023/1114. This information shall include details on:
  - (i) the mechanisms to control, assess and maintain effectively the knowledge and competence of the natural persons providing advice or portfolio management on crypto-assets;
  - (ii) the arrangements to ensure that natural persons involved in the provision of advice or portfolio management are aware of, understand and apply the applicant's internal policies and procedures designed to ensure compliance with Regulation (EU) 2023/1114, especially Article 81(1) of Regulation (EU) 2023/1114 and anti-money laundering and anti-terrorist financing obligations in accordance with Directive (EU) 2015/849;
  - (iii) the amount of human and financial resources planned to be devoted on a yearly basis by the applicant to the professional development and training of the staff providing advice or portfolio management on crypto-assets;
- (b) the arrangements adopted by the applicant to ensure that the natural persons giving advice on behalf of the applicant have the necessary knowledge and expertise to conduct the suitability assessment referred to in Article 81(1) of Regulation (EU) 2023/1114.

#### *Article 17*

### **Transfer services**

An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 and intending to provide transfer services for crypto-assets on behalf of clients shall provide to the competent authority all of the following information:

- (a) details on the types of crypto-assets for which the applicant intends to provide transfer services;
- (b) the policies and procedures and a detailed description of the arrangements put in place by the applicant to ensure compliance with Article 82 of Regulation (EU) 2023/1114, including detailed information on the applicant's arrangements and deployed ICT and human resources to address risks promptly, efficiently and thoroughly during the provision of transfer services for crypto-assets on behalf of clients, considering potential operational failures and cybersecurity risks;
- (c) if any, a description of the applicant's insurance policy, including on the insurance's coverage of detriment to client's crypto-assets that may result from cyber security risks;
- (d) arrangements to ensure that clients are adequately informed about the policies and procedures and arrangements referred to in point (b).

*Article 18*

**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]*

## 6.6 Annex VI – Draft ITS pursuant to Article 62(6) 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 standard forms, templates and procedures for the information to be included in the application for the authorisation of crypto-asset service providers**

**(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

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

Having regard to the 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 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>22</sup>, and in particular Article 62(6), third subparagraph thereof,

Whereas:

- (1) It is appropriate to set out common standard forms, templates and procedures to ensure a uniform mechanism by which Member States' competent authorities effectively exercise their powers in respect of the application for authorisation as crypto-asset service providers for the provision of crypto-asset services.
- (2) The information submitted by the applicant for authorisation as crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 ('applicant') should be true, accurate, complete and not misleading from the moment of submission of the application until authorisation.
- (3) To facilitate communication between an applicant and the competent authority, competent authorities should designate a contact point specifically for the purpose of the application process and should publish the information on the contact point on their website.
- (4) To ensure a prompt and timely handling of applications for the authorisation of crypto-asset service providers, the competent authority should confirm the receipt of the

---

<sup>22</sup>

OJ L 150, 9.6.2023, p. 40-205.

application by sending electronically, on paper, or in both forms, an acknowledgement of receipt in writing to the applicant. That acknowledgement of receipt shall include the contact details of the persons or function in charge of handling the application for authorisation.

- (5) To allow the competent authority to base its assessment of the application for authorisation on accurate information, applicants should communicate to the competent authority changes to the information provided in the application for authorisation that may affect the outcome of the assessment of such application, without undue delay. Furthermore, it is necessary to establish that the time limits for the assessment of the information laid down in Article 63(9) of Regulation (EU) 2023/1114 apply from the date on which the amended material information is provided by the applicant to the competent authority.
- (6) The competent authority should retain the right to request additional information from the applicant during the assessment process in accordance with the criteria and timelines set out in Regulation (EU) 2023/1114.
- (7) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA'), in close cooperation with the European Banking Authority.
- (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>(23)</sup>,

HAS ADOPTED THIS REGULATION:

### *Article 1*

#### **Designation of a contact point**

Competent authorities shall designate a contact point for receiving the applications for authorisation as a crypto-asset service provider pursuant to Article 62 of Regulation (EU) 2023/1114. Competent authorities shall keep the contact details of the designated contact point up-to-date and shall make those contact details public on their websites.

---

<sup>23</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*

### **Submission of the application**

1. An applicant seeking authorisation as a crypto-asset service provider in accordance with Article 62 of Regulation (EU) 2023/1114 shall submit to the competent authority its application by filling in the form set out in the Annex.
2. The application shall be provided in a manner which enables storage of information in a way accessible for future reference and which allows the unchanged reproduction of the information stored.

## *Article 3*

### **Receipt of the application and acknowledgement of receipt**

The competent authority shall send electronically, on paper, or in both forms, an acknowledgement of receipt in writing to the applicant. That acknowledgement of receipt shall include the contact details of the department, function or staff member of the competent authority handling the application.

## *Article 4*

### **Notification of changes**

1. The applicant shall notify the competent authority of any changes to the information provided in the application for authorisation that could affect the assessment of such application without undue delay. The applicant shall provide the updated information by using the form set out in the Annex.
2. Where the applicant provides updated information in accordance with the previous paragraph, the time limit laid down in Article 63(9) of Regulation (EU) 2023/1114 shall start to run from the date on which that updated information is received by the competent authority.
3. Crypto-asset service providers shall notify the competent authority of any changes to the information on which basis the authorisation was obtained and that could affect such authorisation.

*Article 5*

**Communication of the decision**

The competent authority shall inform the applicant of its decision to grant or not the authorisation in paper form, by electronic means or both.

*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*

*On behalf of the President*

*[Position]*



**ANNEX**

**Application Form for authorisation as a Crypto-Asset Service Provider**

**Regulation (EU) 2023/1114**

Reference number:

Date:

FROM:

Name of the applicant:

Address:

(Contact details of the designated contact person):

Name:

Telephone:

Email:

TO:

Member State (if applicable):

Competent Authority:

Address:

(Contact details of the designated contact point):

Name:

Telephone:

Email:

Dear [*insert appropriate name*],

In accordance with Article 2 of the Commission Implementing Regulation (EU) XXXX/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 standard forms, templates and procedures for the information to be included in the application for the authorisation of crypto-asset service providers, kindly find attached the application for authorisation.

We [applicant] declare that the submitted information is true, accurate, complete and not misleading. Unless specifically stipulated otherwise, the information is up to date on the date of this application.

Information indicating a future date is explicitly identified in the application and we undertake to notify the authority in writing without delay if any such information should turn out to be untrue inaccurate, incomplete or is misleading.

- Person in charge of preparing the application:

Name:

Status/position:

Telephone:

Email:

- Nature of the application (tick the relevant box)

- Authorisation
  
- Notification of changes pursuant to Article 4(3) of Implementing Regulation (EU) XXXX/XXXX of [date]

#### REQUIRED INFORMATION

##### *General information*

.....  
.....

Please insert the information referred to under Article 1 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

##### *Programme of operations*

.....  
.....

Please insert the information referred to under Article 2 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by

setting out that information here or making reference to the relevant sections of the application.

*Prudential requirements*

.....  
.....

Please insert the information referred to under Article 3 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Information about governance arrangements and internal control mechanisms*

.....  
.....

Please insert the information referred to under Article 4 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Business continuity*

.....  
.....

Please insert the information referred to under Article 5 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by

setting out that information here or making reference to the relevant sections of the application.

*Detection and prevention of money laundering and terrorist financing*

.....  
.....

Please insert the information referred to under Article 6 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Identity and proof of good repute, knowledge, skills, and experience and of sufficient time commitment of the members of the management body*

.....  
.....

Please insert the information referred to under Article 7 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Information relating to shareholders or members with qualifying holdings*

.....  
.....

Please insert the information referred to under Article 8 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by

setting out that information here or making reference to the relevant sections of the application.

*ICT systems and related security arrangements*

.....  
.....

Please insert the information referred to under Article 9 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Segregation of clients' crypto-assets and funds*

.....  
.....

Please insert the information referred to under Article 10 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Complaints-handling*

.....  
.....

Please insert the information referred to under Article 11 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by

setting out that information here or making reference to the relevant sections of the application.

*Custody and administration policy*

.....  
.....

Please insert the information referred to under Article 12 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Operating rules of the trading platform and market abuse detection*

.....  
.....

Please insert the information referred to under Article 13 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Exchange of crypto-assets for funds or other crypto-assets*

.....  
.....

Please insert the information referred to under Article 14 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by

setting out that information here or making reference to the relevant sections of the application.

*Execution policy*

.....  
.....

Please insert the information referred to under Article 15 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Provision of advice or portfolio management on crypto-assets*

.....  
.....

Please insert the information referred to under Article 16 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by setting out that information here or making reference to the relevant sections of the application.

*Transfer services*

.....  
.....

Please insert the information referred to under Article 17 of Commission Delegated Regulation (EU) XXXX/XXXX of [date - MiCA RTS on authorisation for CASPs], by



setting out that information here or making reference to the relevant sections of the application.

Yours sincerely,

[signature]

## 6.7 Annex VII – Draft RTS pursuant to Article 71(5) 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 on the requirements, templates and procedures for handling complaints**

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 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>24</sup>, and in particular Article 71(5), third subparagraph, thereof,

Whereas:

- (1) In the interests of investor protection, crypto-asset service providers should provide their clients with easy access to a clear, understandable and up-to-date description of their complaints-handling procedure on their website.
- (2) In order to avoid diverging complaints handling procedures among crypto-asset service providers across the Union, clients should be able to file their complaints using a harmonised template. To ensure maximum flexibility for clients to file their complaints, the use of such template should not be deemed mandatory.
- (3) In order to provide for an adequate level of protection of investors, crypto-asset service providers should publish a description of the complaints handling procedure and the standard template set out in the Annex in all languages used by the crypto-assets service provider to market its services or communicate with clients. In addition, it is necessary to ensure that complaints may be filed in the languages used by the crypto-assets service provider to market its services or communicate with clients, as well as in the official languages of the home Member State and host Member States that are also official languages of the Union.
- (4) To ensure a prompt and timely handling of complaints, crypto-asset service providers should acknowledge receipt of any complaint without undue delay. Crypto-asset service providers should also, without undue delay, inform the complainant as to whether that complaint is admissible or not and, in the latter case, communicate the reasons for the

---

<sup>24</sup>

OJ L 150, 09.06.2023, p.40-205.

inadmissibility. Upon acknowledgment of receipt of the complaint, the complainant should also receive the contact details of the person or department to be contacted for any queries related to the complaint, as well as an indicative timeframe for a response.

- (5) To ensure a prompt, timely and fair investigation of complaints, crypto-asset service providers should, upon receipt of a complaint, assess whether that complaint is clear, complete and contains all relevant information necessary for handling it. Where appropriate, additional information should be requested without undue delay. Crypto-asset services providers should gather and investigate all relevant information regarding the complaint. Complainants should be kept duly informed about the complaints handling process.
- (6) To ensure a fair and effective handling of complaints, it is necessary that decisions on complaints address all points raised by the complainant in its complaint. Moreover, complaints presenting similar circumstances should result in consistent decisions, unless the crypto-asset service provider is able to provide an objective justification for any possible deviation from a previously taken decision.
- (7) To ensure a prompt handling of complaints, decisions on complaints should be communicated to the complainant without undue delay, within the timeframe determined in the complaints handling procedure and in any case within 2 months of the date the complaint was received by the crypto-asset service provider. In exceptional circumstances where the crypto-asset service provider is not able to comply with the timeframe determined in the complaints handling procedure or to meet two-month deadline, the complainant should, without undue delay, be informed of the reasons for the delay and of the expected date by which a decision will be delivered.
- (8) In order to ensure efficient interactions, crypto-asset service providers should communicate with complainants in clear and plain language that clients can easily understand. Communications of crypto-asset service providers should be made in writing by electronic means or, upon the complainant's request, in paper form. Where the decision on a complaint does not address positively all of the complainant's request, the decision should contain a thorough reasoning and information on available remedies, to enable clients to pursue further action if they do not agree with the reasons for the rejection.
- (9) In order to achieve procedural and substantive consistency of complaints handling, crypto-asset service providers should analyse complaints-handling data on an ongoing basis, including inter alia, the average processing time, per year (on a rolling basis), for each step of the complaints handling procedure.
- (10) To ensure that complaints are investigated fairly and effectively, adequate resources should be dedicated by the crypto-asset service provider to their management. Such resources should also ensure that complaints are handled without conflicts of interests. To ensure an adequate level of visibility and responsibility at a high level of the organisation, the complaints-handling policies and procedures should be defined and endorsed by the management body, which shall also be responsible for monitoring their

proper implementation and for their periodical review, in accordance with Article 68(6) of MiCA.

- (11) Any processing of personal data under this Regulation should be carried out in accordance with applicable Union law on the protection of personal data. This Regulation is without prejudice to the rights and obligations under Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>25</sup>.
- (12) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Securities and Markets Authority ('ESMA'), in close cooperation with the European Banking Authority.
- (13) 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>26</sup>.

HAS ADOPTED THIS REGULATION:

### *Article 1*

#### **Complaints-handling procedures**

1. For the purposes of this Regulation, 'complaint' means a statement of dissatisfaction addressed to a crypto-asset service provider by one of its clients relating to the provision of one or more crypto-asset services.
2. The procedures for complaints handling as referred to in Article 71(1) of Regulation (EU) 2023/1114 shall contain at least all of the following information:
  - (a) the conditions for the admissibility of complaints;
  - (b) information that complaints are filed and handled free of charge;

---

<sup>25</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).

<sup>26</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).

- (c) a detailed description of how to file complaints, including:
  - (i) information that complaints may be filed using the template set out in the Annex;
  - (ii) the type of information to be provided by the complainant;
  - (iii) the identity and contact details of the person to whom or department to which complaints must be addressed;
  - (iv) the electronic platform, system, email or postal address to which complaints must be submitted;
  - (v) the language or languages in which a complainant is allowed to file a complaint pursuant to Article 3;
- (d) the process for complaints handling, as specified in Articles 3 to 6;
- (e) the timeline applicable to complaint handling, including for acknowledging receipt of the complaint, requesting additional information, investigating a complaint and providing a response;
- (f) a description of the arrangements for registering and keeping records of complaints and of measures taken in response thereto through a secure electronic system.

3. Crypto-asset service providers shall publish an up-to-date description of the procedures for complaints handling on their website, as well as the standard template set out in the Annex, and ensure that both the description and the template are easily accessible on their website and on any other relevant digital device that may be used by clients to access the crypto-asset services. In addition, they shall provide such description upon clients' request and at the time of acknowledging receipt of complaints.

4. The description of the complaints handling procedure and the standard template set out in the Annex shall be published in all languages used by the crypto-assets service provider to market its services or communicate with clients. P

5. The crypto-asset service provider shall adequately document the procedures for complaints handling and shall communicate such procedures to all relevant staff through an adequate internal channel and provide appropriate training.

6. The crypto-asset service provider shall ensure that the procedures for complaints handling are defined and endorsed by its management body, which shall also be responsible for monitoring their proper implementation.

7. The crypto-asset service provider shall ensure that the conditions a complaint shall meet to be considered admissible and complete are fair, reasonable and do not unduly restrict the

rights of natural or legal persons to file a complaint. Such conditions shall not include the mandatory use of the template provided in the Annex to this Regulation.

## *Article 2*

### **Resources dedicated to complaints-handling**

1. Crypto-asset service providers shall dedicate adequate resources to the management of complaints.
2. The dedicated resources referred to in paragraph 1 shall have access to all relevant information.
3. The person in charge of the dedicated resources referred to in paragraph 1 shall report directly to the management body on the implementation and effectiveness of the complaints handling procedures, including the data referred to in Article 8, and on any measures taken or to be taken in response thereto.

## *Article 3*

### **Submission means and language**

1. Crypto-asset service providers shall ensure that clients are able to submit complaints by electronic means or in paper form.
2. Crypto-asset service providers shall ensure that clients are able to file complaints in:
  - (a) the languages used by the crypto-assets service provider to market its services or communicate with clients;
  - (b) the official languages of the home Member State and host Member States that are also official languages of the Union.

#### *Article 4*

##### **Acknowledgment of receipt and verification of admissibility**

1. Crypto-asset service providers shall acknowledge receipt of a complaint and inform the complainant about whether the complaint is admissible without undue delay after its receipt.
2. Where a complaint does not fulfil the conditions of admissibility referred to in Article 1(2) and (7), crypto-asset service providers shall provide the complainant with a clear explanation of the reasons for rejecting the complaint as inadmissible.
3. The acknowledgment of receipt of a complaint shall contain all of the following:
  - (a) the identity and contact details, including email address and telephone number, of the person to whom, or the department to which, complainants can address any query related to their complaint;
  - (b) the date of receipt of the complaint;
  - (c) a reference to the timeline referred to in Article 1(2), point (e);
  - (d) where an electronic complaint form is filed, a copy of the complaint filed by the client.

#### *Article 5*

##### **Investigation of complaints**

1. Upon receipt of an admissible complaint, crypto-asset service providers shall, without undue delay after acknowledging receipt of the complaint, assess whether the complaint is clear and complete. In particular, they shall assess whether the complaint contains all relevant information. Where a crypto-asset service provider concludes that a complaint is unclear or incomplete, it shall request any additional information necessary for the proper handling of the complaint.
2. Crypto-asset service providers shall seek to gather and examine all relevant information regarding a complaint. They shall not require from the complainant information that is already in their possession or that should be in their possession.
3. Crypto-asset service providers shall keep the complainant duly informed about any additional steps taken to handle the complaint. They shall reply to reasonable information requests made by the complainant without any undue delay.

## *Article 6*

### **Decisions**

1. In its decision on a complaint, the crypto-asset service provider shall address all points raised in the complaint and shall state the reasons for the outcome of the investigation. That decision shall be consistent with any previous decision taken by the crypto-asset service provider in respect of similar complaints, unless the crypto-asset service provider is able to justify why a different conclusion is drawn.
2. Crypto-asset service providers shall communicate their decision on a complaint to the complainant without undue delay, within the timeline referred to in Article 1(2), point (e) and in any case within 2 months of the date the complaint is received by the crypto-asset service provider.
3. Where, in exceptional situations, the decision on a complaint cannot be provided within the timeline referred to in of Article 1(2), point (e) or deadline referred to in paragraph 2, crypto-asset service providers shall inform the complainant without undue delay about the reasons for that delay and specify the date of the decision.
4. Where the decision does not satisfy the complainant's demand or only partly satisfies it, the crypto-asset service provider shall clearly set out the reasoning and contain information on available remedies.

## *Article 7*

### **Communication with clients**

1. When handling complaints, crypto-asset service providers shall communicate with complainants in a clear and plain language that is easy for clients to understand.
2. Any communication made by the crypto-asset service provider under Articles 4 to 6 that is addressed to a complainant shall be made in the language in which the complainant filed its complaint, provided that the language used by the complainant is one of the languages referred to in Article 3(2). The communication shall be made in writing by electronic means, or upon the complainant's request, in paper form.



*Article 8*

**Procedures to ensure consistent complaints-handling**

Crypto-asset service providers shall analyse, on an ongoing basis, complaints-handling data. Such data shall include all of the following:

- (a) the average processing time, for the relevant period under consideration, for each step of the complaints handling procedure, including acknowledgement, investigation, response time;
- (b) the number of complaints received, for the relevant period under consideration, and for each step of the complaints handling procedure, the number of complaints where the crypto asset service provider did not comply with the maximum time limits set out in its complaints handling procedure;
- (c) the categories of the topics to which complaints relate;
- (d) outcomes of investigations.

*Article 9*

**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 submission of complaints**

<p><b>SUBMISSION OF A COMPLAINT</b></p> <p>(to be sent by the client to the crypto-asset service provider)</p>
--

*1.a. Personal data of the complainant*

LAST NAME/LEGAL ENTITY NAME	FIRST NAME	REGISTRATION or ID NUMBER	LEI (IF AVAILABLE)	CLIENT REFERENCE (IF AVAILABLE)

ADDRESS:  STREET, NUMBER, FLOOR  (for firms registered office)	POSTCODE	CITY	COUNTRY

TELEPHONE		EMAIL	
-----------	--	-------	--

*1.b Contact details (if different from 1.a)*

LAST NAME/LEGAL ENTITY NAME	FIRST NAME

ADDRESS: STREET, NUMBER, FLOOR (for firms registered office)	POSTCODE	CITY	COUNTRY

TELEPHONE		EMAIL	

*2.a Personal data of the legal representative (if applicable) (a power of attorney or other official document as proof of the appointment of the representative)*

LAST NAME	FIRST NAME/LEGAL ENTITY NAME	REGISTRATION NUMBER AND LEI (IF AVAILABLE)

ADDRESS: STREET, NUMBER, FLOOR (for firms registered office)	POSTCODE	CITY	COUNTRY

TELEPHONE	EMAIL

*2.b Contact details (if different from 2.a)*

LAST NAME/LEGAL ENTITY NAME	FIRST NAME

ADDRESS: STREET, NUMBER, FLOOR (for firms registered office)	POSTCODE	CITY	COUNTRY

TELEPHONE	EMAIL

**3. Information about the complaint**

*3.a Full reference of the crypto-asset service or agreement to which the complaint relates (i.e. name of the crypto-asset service provider, crypto-asset service reference number, or other references of the relevant transactions...)*

*3.b Description of the complaint's subject-matter*

Please provide documentation supporting the facts mentioned.

*3.c Date(s) of the facts that have led to the complaint*

*3.d Description of damage, loss or detriment caused (where relevant)*

*3.e Other comments or relevant information (where relevant)*

In \_\_\_\_\_ (place) on \_\_\_\_\_ (date)

*SIGNATURE*

**COMPLAINANT/LEGAL REPRESENTATIVE**

*Documentation provided (please check the appropriate box):*

<i>Power of attorney or other relevant document</i>	
<i>Copy of the contractual documents of the investments to which the complaint relates</i>	
<i>Other documents supporting the complaint:</i>	

## 6.8 Annex VIII – Draft RTS pursuant to Article 84 (4) of MiCA

### COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

**supplementing Regulation EU (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a crypto-asset service provider**

**(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 1093/2012 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937<sup>27</sup>, and in particular Article 84(4), third subparagraph, thereof,

Whereas:

- (1) Detailed information should be required from a proposed acquirer of a qualifying holding, direct or indirect, in a crypto-assets services provider authorised in accordance with Article 63 of Regulation (EU) 2023/1114 (“target entity”) at the time of the initial notification to enable competent authorities, within the meaning of point (35)(a) of Article 3(1) of Regulation (EU) 2023/1114 to carry out the prudential assessment of the proposed acquisition, proportionate and adapted to the nature of the proposed acquirer and the proposed acquisition. Information on the identity of the proposed acquirer and of the persons who will direct the business should be provided by the proposed acquirer irrespective of whether it is a natural or a legal person, in order to enable the competent authority of the target entity to assess the reputation of that proposed acquirer.
- (2) The information contained in the notification submitted by the proposed acquirer should be true, accurate, complete and up-to-date from the moment of submission of the notification until the completion of the assessment by the competent authority. For that

---

<sup>27</sup> OJ L 150, 9.6.2023, p. 40.

purpose, competent authorities should be informed of any changes to the information provided in the notification.

- (3) The notification should contain data about the proposed acquirer including the members of their management body, the indirect shareholders and the ultimate beneficial owner, and of the members of the management body of the target entity in case the proposed acquirer intends to appoint any. That information would include personal data. In compliance with the principle of data minimisation enshrined in Article 5(1), point (c) of Regulation (EU) 2016/679 of the European Parliament and of the Council<sup>28</sup>, such personal data should be necessary and sufficient to enable the competent authority to thoroughly assess the criteria laid down in Article 84(1), points (a) to (e) of Regulation (EU) 2023/1114. When assessing the notification of the proposed acquisition and processing the personal data included therein, competent authorities should comply with the relevant provisions of Regulation (EU) 2016/679. Furthermore, in pursuance of data protection principles, such personal data should be kept by the competent authority for no longer than it is necessary to the performance of its supervisory tasks. Information on the identity of the proposed acquirer should be provided by the proposed acquirer irrespective of whether it is a natural or a legal person, in order to enable the competent authority of the target entity to assess the reputation of that proposed acquirer.
- (4) Where the proposed acquirer is a legal person, information on the identity of the ultimate beneficial owners and on the reputation and experience, over the last ten years, of the persons who effectively direct the business of the proposed acquirer is also necessary to perform the prudential assessment.
- (5) Where the proposed acquirer is or is intended to be a trust structure, it is necessary for the competent authority of the target entity to obtain information on both the identity of the trustees who will manage the assets of the trust, and on the identity of the settlor and of the beneficial owners of those assets to be able to assess the reputation and experience of these persons.
- (6) Similarly, where the proposed acquirer is an alternative investment fund (AIF), as defined in point (a) of Article 4(1) of Directive 2011/61/EU of the European Parliament and of the Council<sup>29</sup> or an undertaking for collective investment in transferable securities (UCITS), authorised in accordance with Article 5 of Directive 2009/65/EC of the European

---

<sup>28</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).

<sup>29</sup> Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 (OJ L 174, 1.7.2011, p. 1).



Parliament and of the Council<sup>30</sup>, its alternative investment fund manager (AIFM) or the AIF in the case of an internally- managed AIF, or its UCITS management company or the UCITS investment company in the case of a self-managed UCITS, should provide the competent authority of the target entity with the identity and information necessary for the assessment of the reputation of the individuals in charge of making the investment decisions for the fund.

- (7) Where the proposed acquirer is a sovereign wealth fund, it should provide the competent authority with comprehensive information relevant to the assessment of reputation. This should include information on the identity and reputation of the persons holding high level positions in the ministry, government department or other public body in charge of making the investment decisions for the fund.
- (8) Where the proposed acquirer is a natural person, it is necessary to obtain information both in relation to the proposed acquirer and in relation to any undertaking formally directed or controlled by the proposed acquirer over the last ten years in order to provide the competent authority of the target entity with full information relevant to the assessment of reputation.
- (9) Where the proposed acquirer is a legal person, it is necessary to obtain information in relation to any undertaking under the proposed acquirer's control, and any shareholder with a qualifying holding in the proposed acquirer, in order to provide the competent authority with full information relevant to the assessment of reputation.
- (10) The information relevant to the assessment of reputation should include details of criminal convictions and of pending criminal proceedings and civil or administrative cases, open investigations and proceedings, sanctions or other enforcement decisions against the proposed acquirer relating to commercial law, insolvency law, financial services law, money laundering, and terrorist financing, fraud or professional liability, as well as any other relevant information such as refusal of registration or dismissal from employment or from a position of trust which is deemed relevant in order to assess the reputation of the proposed acquirer.
- (11) Information on whether an assessment as acquirer, or as a person who directs the business of any relevant entity has already been conducted by another competent authority or other authority, and, if so, the outcome of such assessment should be provided by the proposed acquirer, in order to ensure that the outcome of investigations

---

<sup>30</sup> Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (recast) (OJ L 302, 17.11.2009, p. 32).

run by other authorities are duly considered by the competent authority of the target entity when conducting its own assessment of the proposed acquirer.

- (12) In order to facilitate the retrieval of previous assessments in supervisory databases and facilitate cooperation among competent authorities, the proposed acquirer should submit the legal entity identifier with the information included in the notification to the competent authority. The legal entity identifier is a unique international identifier for an unambiguous and consistent identification of proposed acquirers. In contrast to national codes or names of legal entities, the legal entity identifier is a widely recognised and financially accessible international identifier suited for overseeing entities in multiple jurisdictions.
- (13) With regard to the proposed acquisition of indirect qualifying holdings in the target entity, it is adequate to calibrate in a proportionate way the content of the information request. For this purpose, it is relevant to differentiate two cases. The first one is the case where the natural or legal person indirectly acquiring or increasing a qualifying holding in the target entity holds or intends to acquire the control of an existing holder of qualifying holdings in the target entity. The second is the case where the existence of a qualifying holding is determined by multiplying the qualifying holding held in the target entity by the percentage of the qualifying holdings held indirectly along the holding chain. In the second case, having regard to the more limited influence that such an indirect shareholder or member with qualifying holdings may exercise on the target entity, a reduced set of information should be submitted.
- (14) Proposed acquirers might envisage the appointment of one or more members of the management body of the target entity. In order for the competent authority to be able to assess new members of the management body of the target entity, the proposed acquirer should provide the same information which is required from members of management bodies of crypto-asset service providers at the moment of authorisation.
- (15) Financial information concerning the proposed acquirer, including a description of the current business activities of the proposed acquirer, should be provided in order to assess the financial soundness of that proposed acquirer.
- (16) It is important for the competent authority of the target entity to assess whether the existence of any potential conflict of interests could affect the financial soundness of the proposed acquirer and the sound and prudent management of the target entity. Therefore, proposed acquirers should provide information on the financial and non-financial interests or relationships of the proposed acquirer with any shareholders or directors or members of the management body of the target entity or person entitled to exercise voting rights in the target entity, or with the target entity itself or its group.

- (17) The submission of additional information is necessary when the proposed acquirer is a legal person. This should allow the competent authority of the target entity to complete the assessment of the proposed acquisition, including in cases where the legal and group structures involved may be complex and may necessitate detailed review in relation to reputation, potential action in concert with other parties, and the ability of the competent authority of the target entity to continue effective supervision of the target entity.
- (18) Where the proposed acquirer is an entity established in a third country or is part of a group whose direct or ultimate parent undertaking is established outside the Union, additional information should be provided so that the competent authority of the target entity can assess whether there are obstacles to the effective supervision of the target entity posed by the legal regime of the third country, and can also ascertain the proposed acquirer's reputation in that third country.
- (19) Specific information enabling an assessment as to whether the proposed acquisition will impact the ability of the competent authority of the target entity to carry out effective supervision of the target entity should be submitted by the proposed acquirer. For legal persons, it is necessary to assess the impact of the proposed acquisition on the consolidated supervision of the target entity and of the group it would belong to after the acquisition.
- (20) The assessment of the proposed acquisition requires the proposed acquirer to provide information identifying the target entity, providing details on the proposed acquirer's intention and strategic investment as well as on the shares owned or contemplated to be owned by the proposed acquirer. This information should include details of any action undertaken by the proposed acquirer in concert with other parties for the purposes of the proposed acquisition, the information about the price of the proposed acquisition and a copy of the contract of acquisition should also be provided.
- (21) Furthermore, the proposed acquirer should provide information on the financing of the proposed acquisition, including information concerning all means and sources of financing. The proposed acquirer should also be able to present evidence about the origin and legitimacy of the source of all such funds and assets, including any crypto-asset or other digital asset, in order for the competent authority of the target entity to assess their certainty, sufficiency and legitimate origin, including whether there is a risk of money laundering or terrorist financing.
- (22) Proposed acquirers intending to acquire a qualifying holding of more than 20% and up to 50% in the target entity should provide information on their strategy to the competent authority of the target entity in order to ensure a comprehensive assessment of the proposed acquisition. Similarly, proposed acquirers intending to acquire a qualifying holding of less than 20% in the target entity but exercising an equivalent significant

influence over it through other means, such as the relationships between the proposed acquirer and the existing shareholders, the existence of shareholders' agreements, the distribution of shares, participating interests and voting rights across shareholders or the proposed acquirer's position within the group structure of the target entity, should also provide that information to ensure a high degree of homogeneity in assessing proposed acquisitions.

- (23) Where there is a proposed change in control of the target entity, the proposed acquirer should, as a general rule, submit a full business plan. However, where there is no proposed change in the control of the target entity, it should be sufficient to be in possession of certain information on the entity's future strategy and the proposed acquirer's intentions for the target entity in order to assess whether this will not affect the financial soundness of the proposed acquirer.
- (24) Having regard to the principle of proportionality, in certain cases, the proposed acquirer should submit reduced information. Namely, where the proposed acquirer has been assessed for acquisition or increase in qualifying holdings by the same competent authority of the target entity within the previous two years, it should be required to submit only the information that has changed since the previous assessment. Similarly, where the proposed acquirer is an authorised undertaking and subject to the prudential supervision of the same competent authority of the target entity, it should be exempted from submitting certain pieces of information that are already in the possession of such competent authority. In both cases, the proposed acquirer should only submit information specific to the proposed acquisition together with a signed declaration certifying that the rest of the information set-out in this Regulation that has not been submitted because in possession of the competent authority is true, accurate and up-to-date.
- (25) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority to the European Commission. The European Securities and Markets Authority has developed these draft regulatory technical standards in close cooperation with the European Banking Authority.
- (26) The European Securities and Markets Authority has conducted an open public consultation 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>31</sup>,

---

<sup>31</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*

**General information relating to the proposed acquirer**

1. The proposed acquirer that is a natural person shall provide the competent authority of the target entity with the following identification information:

(a) personal details, including all of the following:

- (i) the person's name and, if different, the person's name at birth;
- (ii) the date and place of birth;
- (iii) the person's nationality or nationalities;
- (iv) the person's personal national identification number, where available;
- (v) the person's current place of residence, address and contact details, and any other place of residence in the past ten years;
- (vi) a copy of an official identity document;
- (vii) the name and contact details of the principal professional adviser, if any, used to prepare the notification;

(b) detailed curriculum vitae, stating the relevant education and training, and any professional experience in managing holdings in companies, any management experience, any professional activities or other relevant functions currently performed, and any previous professional experience relevant to financial services, crypto-assets or other digital assets, distributed ledger technology ('DLT'), information technology, cybersecurity, digital innovation;

2. The proposed acquirer that is a legal person shall provide the competent authority of the target entity with the following information:

(a) the name of the legal person;

(b) the name and contact details of the principal professional adviser, if any, used to prepare the application;

- (c) where the legal person is registered in a central register, commercial register, companies register or similar public register, the name of the register in which the legal person is entered, the registration number or an equivalent means of identification in that register and a copy of the registration certificate;
- (d) the validated, issued and duly renewed ISO 17442 legal entity identifier released in accordance with the terms of any of the accredited Local Operating Units of the Global Legal Entity Identifier System;
- (e) the addresses of the legal person's registered office and, where different, of its head office, and principal place of business;
- (f) contact details of the person within the proposed acquirer to contact regarding the notification;
- (g) corporate documents or agreements governing the legal person and a summary explanation of the main legal features of the legal form of the legal person as well as an up-to-date overview of its business activity;
- (h) whether the legal person has ever been or is regulated by a competent authority in the financial services sector or other government body and the name of such authority or other government body;
- (i) where the legal person is an obliged entity within the meaning of Article 2 of Directive (EU) 2015/849 of the European Parliament and of the Council<sup>32</sup>, the applicable anti-money laundering and counter terrorist-financing policies and procedures;
- (j) a complete list of the persons who effectively direct the business of the proposed acquirer and, in respect of each such person, the name, date and place of birth, address, contact details, a copy of the official identity document, the national identification number where available, the detailed curriculum vitae stating relevant education and training, the previous professional experience, and the professional activities or other relevant functions currently performed, including professional experience in managing holdings in companies, in financial services, crypto-assets or other digital assets, distributed ledger technology (DLT), information technology, cybersecurity or digital innovation, together with the information referred to in points (a) and (b) of Article 2;

---

<sup>32</sup> Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

(k) the identity of all persons who are the legal person's ultimate beneficial owners, in accordance with Article 3(6)(a)(i) or 3(6)(c) of Directive (EU) 2015/849, in respect of each such person, the name, date and place of birth, address, contact details, and, where available, the national identification number, together with the information referred to in points (a) and (b) of Article 2.

3. The proposed acquirer that is a trust shall provide the competent authority of the target entity with the following information:

- (a) the identity of all trustees who manage assets under the terms of the trust document. In respect of each such person, their date and place of birth, address, contact details, a copy of their official identity document, their national identification number where available, their detailed curriculum vitae stating relevant education and training, their previous professional experience, and their professional activities or other relevant functions currently performed, including professional experience in managing holdings in companies, in financial services, crypto-assets or other digital assets, distributed ledger technology (DLT), information technology, cybersecurity or digital innovation, together with the information referred to in points (a) and (b) of Article 2;
- (b) the identity, including the date and place of birth, address, contact details, copy of the official identity document, of each person who is a settlor, a beneficiary or a protector (where applicable) of the trust property and, where applicable, their respective shares in the distribution of income generated by the trust property;
- (c) a copy of any document establishing and governing the trust;
- (d) a description of the main legal features of the trust and its functioning, as well as an up-to-date overview of its business activity, and type and value of the trust property;
- (e) a description of the investment policy of the trust and possible restrictions on investments, including information on the factors influencing investment decisions and the exit strategy in relation to the crypto-asset service provider;
- (f) the information set out in point (i) of paragraph (2).

4. Where the proposed acquirer is an alternative investment fund (AIF) as defined in point (a) of Article 4(1) of Directive 2011/61/EU or an undertaking for collective investment in transferable securities (UCITS) authorised in accordance with Article 5 of Directive 2009/65/EC, its alternative investment fund manager (AIFM) or the AIF in the case of an internally-managed AIF, or its UCITS management company or the UCITS investment company in the case of a self-managed UCITS, shall provide the competent authority of the target entity with the following information:



- (a) details of the investment policy and any restrictions on investments, including information on the factors influencing investment decisions, and of exit strategies;
  - (b) the identity and position of the persons responsible, whether individually or as a committee, for determining and making the investment decisions for the AIF or UCITS, as well as a copy of any contract in case of delegation of portfolio management to a third party or, where applicable, terms of reference of the committee. For each such person the AIFM or UCITS management company, or the AIF or self-managed UCITS investment company shall provide the date and place of birth, address, contact details, a copy of their official identity document, their national identification number where available, their detailed curriculum vitae stating relevant education and training, their previous professional experience, and their professional activities or other relevant functions currently performed, together with the information referred to in points (a) and (b) of Article 2;
  - (c) the information set out in point (i) of paragraph (2);
  - (d) a detailed description of the performance of qualifying holdings previously acquired by the AIFM or UCITS management company on behalf of the AIFs or UCITS they manage, or by the AIF or self-managed UCITS investment company, in accordance with this paragraph in the last three years in other similar firms or in firms providing services in relation to crypto-assets or issuing crypto-assets, indicating whether the acquisition of such qualifying holdings was approved by a competent authority and, if so, the identity of that authority.
5. The proposed acquirer that is a sovereign wealth fund shall provide the competent authority of the target entity with the following information:
- (a) the name of the ministry, government department or other public body in charge of determining the investment policy of the sovereign wealth fund;
  - (b) details of the investment policy of the sovereign wealth fund and any restrictions on investment;
  - (c) the names and positions of the individuals in high level administrative position in the ministry, government department or other public body who are in charge of determining the investment policy and who are responsible for making the investment decisions for the sovereign wealth fund. For each such individual the proposed acquirer shall provide their date and place of birth, address, contact details, a copy of their official identity document, their national identification number where available, their detailed curriculum vitae stating relevant education and training, their previous professional experience, and their professional activities or other relevant functions currently performed, including professional experience in managing holdings in companies, in financial services, crypto-assets or other digital assets, distributed ledger technology (DLT), information technology,



cybersecurity or digital innovation, together with the information referred to in points (a) and (b) of Article 2;

(d) details of any influence exerted by the ministry, government department or other public body referred to in point (a) on the day-to-day operations of the sovereign wealth fund;

(e) the information set out in point (i) of paragraph (2), where applicable.

## *Article 2*

### **Additional information relating to the proposed acquirer that is a natural person**

The proposed acquirer that is a natural person shall also provide the competent authority of the target entity with the following:

(a) a statement containing the following information in respect of the proposed acquirer and of any undertaking directed or controlled by proposed acquirer over the last 10 years:

(i) subject to national legislative requirements concerning the disclosure of spent convictions, information about any criminal conviction or proceedings where the person has been found against and which were not set aside;

(ii) information about any civil or administrative decisions concerning the person that are relevant for the assessment of the acquisition of the qualifying holding in the crypto asset service provider and any administrative sanctions or measures that were imposed as a consequence of a breach of laws or regulations, including disqualification as a company director, in each case which was not set aside and against which no appeal is pending or may be filed, and of criminal convictions in respect of which information shall also be provided for rulings still subject to appeal;

(iii) any bankruptcy, insolvency or similar procedures;

(iv) any pending criminal investigations or procedures including relating to precautionary measures;

(v) any civil, administrative investigations, enforcement proceedings, sanctions or other enforcement decision against the person concerning matters which may reasonably be considered to be relevant to the assessment of the acquisition of the qualifying holding in the crypto asset service provider;

- (vi) where such documents exist, an official certificate or any other equivalent document, where such documents do not exist any reliable source of information concerning the absence of any of the events set out in points (i) to (v) of this point (a) in respect of the person. Official records, certificates and documents shall have been issued within three months before the submission of the notification;
  - (vii) any refusal of registration, authorisation, membership or licence to carry out trade, business or a profession;
  - (viii) any withdrawal, revocation or termination of a registration, authorisation, membership or licence to carry out a trade, business or a profession;
  - (ix) any expulsion by a regulatory or government body or by a professional body or association;
  - (x) any position of responsibility within an entity subject to any criminal conviction or civil or administrative penalty or other civil or administrative measure that is relevant for the assessment of the suitability or authorisation process taken by any authority or any on-going investigation, in each case for conduct failings, including in respect of fraud, dishonesty, corruption, money laundering, terrorist financing or other financial crime or of failure to put in place adequate policies and procedures to prevent such events, held at the time when the alleged conduct occurred, together with details of such occurrences and of the involvement, if any, in them;
  - (xi) any dismissal from employment or a position of trust, any removal from a fiduciary relationship, save as a result of the relationship concerned coming to an end by passage of time, and any similar situation;
- (b) where another supervisory authority has already assessed the person concerned, the identity of that authority, the date of the assessment and evidence of the outcome of this assessment;
- (c) the current financial position of the person, including details concerning sources of revenues, assets and liabilities, security interests and guarantees, whether granted or received;
- (d) a description of the current business activities of the person and of any undertaking which the person directs or controls;
- (e) financial information, including credit ratings and publicly available reports on any undertakings directed or controlled by the person;

- (f) a description of the financial interests of the person, and of any non-financial interests of the person with any of the following natural or legal persons:
- (i) any other current shareholder or member of the target entity;
  - (ii) any person entitled to exercise voting rights of the target entity in any of the following cases or combination of them:
    - voting rights held by a third party with whom that person has concluded an agreement, which obliges them to adopt, by concerted exercise of the voting rights held by them, a lasting common policy towards the management body of the target entity in question;
    - voting rights held by a third party under an agreement concluded with that person providing for the temporary transfer for consideration of the voting rights in question;
    - voting rights attached to shares which are lodged as collateral with that person, provided the person controls the voting rights and declares his or her intention of exercising them;
    - voting rights attached to shares in which that person has the life interest;
    - voting rights which are held, or may be exercised within the meaning of the first four items of this point (ii) by an undertaking controlled by that person;
    - voting rights attaching to shares deposited with that person which the person can exercise at its discretion in the absence of specific instructions from the shareholders;
    - voting rights held by a third party in its own name on behalf of that person;
    - voting rights which that person may exercise as a proxy where the person or entity can exercise the voting rights at its discretion in the absence of specific instructions from the shareholders;
  - (iii) any person that is a member of the management body of the target entity;
  - (iv) the target entity itself or any other member of its group;
- (g) to the extent any conflict of interest arises from the relationships referred to in point (f), proposed methods for managing such conflict;

- (h) a description of any links to politically exposed persons, as defined in Article 3(9) of Directive (EU) 2015/849 of the European Parliament and of the Council<sup>33</sup>;
- (i) any other interests or activities of the person that may be in conflict with those of the applicant and proposed methods for managing those conflicts of interest.

For the purposes of point (f), credit operations, guarantees and security interests, whether granted or received, including relating to crypto-assets or other digital assets, shall be deemed to be part of financial interests, whereas family or close relationships shall be deemed to be part of non-financial interests.

### *Article 3*

#### **Additional information relating to the proposed acquirer that is a legal person**

1. The proposed acquirer that is a legal person shall also provide the competent authority of the target entity with all of the following:

- (a) the information referred to in:
  - (i) Article 2, first subparagraph, point (a), points (i) to (xi) in relation to the legal person and any undertaking under the legal person's control;
  - (ii) Article 2, first subparagraph, point (b) in relation to the legal person itself;
  - (iii) Article 2, first subparagraph, point (d) in relation to the legal person itself;
  - (iv) Article 2, first subparagraph, point (e) in relation to the legal person itself, any member of the management body in their executive function of the legal person or any undertaking under the legal person's control;
- (b) a description of financial interests and non-financial interests or relationships of the proposed acquirer, or, where applicable, the group to which the proposed acquirer belongs, as well as the persons who effectively direct its business with:
  - (i) any other current shareholder or member of the target entity;

---

<sup>33</sup> Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141 of 5.6.2015, p. 73).

- (ii) any person entitled to exercise voting rights of the target entity in any of the following cases or combination of them:
- voting rights held by a third party with whom that person has concluded an agreement, which obliges them to adopt, by concerted exercise of the voting rights held by them, a lasting common policy towards the management of the target entity in question;
  - voting rights held by a third party under an agreement concluded with that person providing for the temporary transfer for consideration of the voting rights in question;
  - voting rights attached to shares which are lodged as collateral with that person, provided the person or entity controls the voting rights and declares its intention of exercising them;
  - voting rights attached to shares in which that person has the life interest;
  - voting rights which are held, or may be exercised within the meaning of the first four items of this point (ii), by an undertaking controlled by that person;
  - voting rights attached to shares deposited with that person which the person can exercise at its discretion in the absence of specific instructions from the shareholders;
  - voting rights held by a third party in its own name on behalf of that person;
  - voting rights which that person may exercise as a proxy where the person can exercise the voting rights at its discretion in the absence of specific instructions from the shareholders;
- (iii) any politically exposed person, as defined in Article 3(9) of Directive (EU) 2015/849;
- (iv) any person that is, according to national legislation, a member of the administrative, management or supervisory body, or of the senior management of the target entity;
- (v) the target entity itself or any other member of its group;
- (c) to the extent any conflict of interest arises from the relationships referred to in point (b), proposed methods for managing such conflicts;

- (d) information on any other interests or activities of the proposed acquirer that may be in conflict with those of the target entity and possible solutions for managing those conflicts of interest;
- (e) the shareholding structure of the proposed acquirer, with the identity of all shareholders exerting significant influence and their respective share of capital and voting rights including information on any shareholders agreements;
- (f) where the proposed acquirer is part of a group, as a subsidiary or as a parent company, a detailed organisational chart of the group structure and information on the activities currently performed by the entities of the group and information on the share of capital and voting rights of shareholders with significant influence of the entities of the group and on the activities currently performed by the entities of the group;
- (g) if the proposed acquirer is part of a group as a subsidiary or as the parent company, information on the relationships between the financial and the non-financial entities of the group;
- (h) identification of any credit institution, payment institution or e-money institution; assurance, insurance or re-insurance undertaking; collective investment undertakings and their managers or investment firm within the group, and the names of the relevant supervisory authorities;
- (i) annual financial statements, at individual level and, where applicable, at consolidated and sub-consolidated levels, for the last three financial years, where the legal person has been in operation for that period of time, or such shorter period of time for which the legal person has been in operation and financial statements were prepared. The proposed acquirer shall submit such financial statements including each of the following items, and where applicable approved by the statutory auditor or audit firm as defined in Article 2, points (2) and (3), of Directive 2006/43/EC of the European Parliament and of the Council<sup>34</sup>:
  - (i) the balance sheet;
  - (ii) the profit and loss accounts or income statements;
  - (iii) the annual reports and financial annexes and any other documents registered with the registry or competent authority of the legal person, including, as set out as relevant in the annual reports, financial annexes and any other registered documents;

---

<sup>34</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (Text with EEA relevance) (OJ L 157, 9.6.2006, p.87).

- (iv) where the proposed acquirer is a newly set-up legal person or entity, in the absence of any financial statements, an updated summary as close as possible to the date of notification, of the financial situation of the proposed acquirer, as well as the financial forecasts for the next three years, and the planning assumptions used in base case and stress scenario.

For the purposes of point (b), credit operations, guarantees and security interests, whether granted or received, including relating to crypto-assets or other digital assets, shall be deemed to be part of financial interests, whereas family or close relationships shall be deemed to be part of non-financial interests.

2. Without prejudice to paragraph 1, where the proposed acquirer that is a legal person has its head office in a third country, it shall also provide the competent authority of the target entity, all of the following information:

- (a) where the legal person is supervised by an authority of a third country in the financial services sector:
  - (i) a certificate of good-standing, or equivalent where not available, from such third country authority in relation to the legal person;
  - (ii) general information about the regulatory regime of that third country as applicable to the legal person;
  - (iii) a detailed description of the applicable anti-money laundering and counter-terrorist financing legal framework, including its consistency with the recommendations of the Financial Action Task Force, and of the related procedures applicable to that person;
  - (iv) a declaration by the relevant foreign competent authorities that there are no obstacles or limitations to the provision of information necessary for the supervision of the target entity.

#### *Article 4*

### **Information to be submitted by persons acquiring an indirect qualifying holding in the target entity**

1. A proposed acquirer shall submit the information set out in paragraph (2) where it:

- (a) intends to acquire, directly or indirectly, control within the meaning of Article 2, points (9) and (10) and Article 22 of Directive 2013/34/EU of the European Parliament and of the

Council ('control')<sup>35</sup>, over an existing holder of a qualifying holding in a target entity, irrespective of whether such existing holding is direct or indirect; or

(b) controls, directly or indirectly the proposed direct acquirer of a qualifying holding in a target entity.

2. Where the conditions set out in points (a) or (b) of paragraph 1 are met, the proposed acquirer shall submit the following:

(a) information set out in Article 1, paragraph 1, in Articles 2, 6 and 8, and in Article 9, 10 or 11, as applicable, if the proposed acquirer is a natural person;

(b) information set out in Article 1, paragraphs 2 to 5, as applicable, in Articles 3, 6 and 8, and in Article 9, 10 or 11, as applicable, if the proposed acquirer is a legal person.

3. Where the conditions set out in points (a) and (b) of paragraph 1 are not met, the proposed acquirer shall submit the information set out in paragraph 4 points (a) and (b), where the percentages of the holdings across the corporate chain, starting from the qualifying holding held directly in the target entity, multiplied per the holding in the level immediately above in the corporate chain results in a qualifying holding of 10% or more. The multiplication shall be applied up the corporate chain for so long as the result of the multiplication is 10% or more.

4. Where the proposed acquirer controls a natural or legal person holding a qualifying holding in accordance with the application of paragraph 3, the proposed acquirer shall submit the following:

(a) information set out in Article 1, paragraph 1, Article 2, points (a), (b) to (f) and (h), Article 6, in points (a) to (f), and in Article 8, if the proposed acquirer is a natural person;

(b) information set out in Article 1, paragraph 2, 3, 4 or 5, in Article 3, paragraph (1), point (a), points (i) to (iv), in Article 3, paragraph (1), point (b), point (iii), in Article (3), paragraph 1, points (f) to (i), in Article 3, paragraph 2, in Article 6, point (a) to (f), and in Article 8, if the proposed acquirer is a legal person.

---

<sup>35</sup> Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).



### *Article 5*

#### **Information on the persons that will direct the business of the target entity**

In case the proposed acquirer envisages the appointment of one or more members of the management body of the target entity, the notification shall contain all the information referred to in Article [7] of the [RTS on information for authorisation for applicant crypto-asset service provider] for each such proposed member.

### *Article 6*

#### **Information relating to the proposed acquisition**

The notification relating to the proposed acquisition shall provide the following information:

- (a) identification of the target entity;
- (b) details of the proposed acquirer's intentions with respect to the proposed acquisition, such as strategic investment or portfolio investment;
- (c) information on the shares of the target entity owned, or contemplated to be owned, by the proposed acquirer before and after the proposed acquisition, including:
  - (i) the number and type of shares – whether ordinary shares or other – of the target entity owned, or intended to be acquired, by the proposed acquirer before and after the proposed acquisition, along with the nominal value of such shares;
  - (ii) the share of the overall capital of the target entity that the shares owned, or intended to be acquired, by the proposed acquirer represent before and after the proposed acquisition;
  - (iii) the share of the overall voting rights of the target entity that the shares owned, or contemplated to be owned, by the proposed acquirer represent before and after the proposed acquisition, if different from the share of capital of the target entity;
  - (iv) the market value, in euros and in local currency, of the shares of the target entity owned, or intended to be acquired, by the proposed acquirer before and after the proposed acquisition;
- (d) any action in concert with other parties, including the contribution of those other parties to the financing of the proposed acquisition, the means of participation in the financial arrangements and future organisational arrangements;

- (e) the content of intended shareholder's agreements with other shareholders in relation to the target entity;
- (f) the proposed acquisition price and the criteria used when determining such price and, if there is a difference between the market value and the proposed acquisition price, an explanation as to why that is the case;
- (g) copy of the contract of acquisition.

#### *Article 7*

##### **Information on the new proposed group structure and its impact on supervision**

1. The proposed acquirer that is a legal person shall provide the competent authority of the target entity with an analysis of the perimeter of consolidated supervision of the group which the target entity would belong to after the proposed acquisition. That analysis shall include information about which group entities would be included in the scope of consolidated supervision requirements after the proposed acquisition and at which levels within the group those requirements would apply on a full or sub-consolidated basis.
2. The proposed acquirer shall also provide the competent authority of the target entity with an analysis of the impact of the proposed acquisition in any way, including as a result of close links of the proposed acquirer with the target entity, and on the ability of the target entity to continue to provide timely and accurate information to its competent authority.

#### *Article 8*

##### **Information relating to the financing of the proposed acquisition**

1. The proposed acquirer shall provide the competent authority of the target entity a detailed explanation of the specific sources of funding for the proposed acquisition, enabling to prove their legitimate origin, certainty and sufficiency, including:
  - (a) detailed description of the activity that generated the funds and assets for the acquisition, supported by relevant documents such as financial statements, bank statements, tax statements and any other document or information providing evidence to the competent authority that no money laundering or terrorist financing is attempted through the proposed acquisition;

- (b) details on any assets, including any crypto-assets, which are to be sold to help finance the proposed acquisition, such as conditions of sale, price, appraisal and details about the characteristics of those assets, including information on when, how and from whom they were acquired;
- (c) details on access to capital sources and financial markets including details of financial instruments to be issued;
- (d) if the funds used for the acquisition of the holding have been borrowed, information on the use of borrowed funds including the name of relevant lenders and details of the facilities granted, including maturities, terms, pledges and guarantees, as well as information on the source of revenue to be used to repay such borrowings;
- (e) details on the means of payment to transfer the funds and assets from the proposed acquirer to the proposed seller to purchase the holding enabling to reconstruct the transfers in line with Regulation (EU) 2023/1113 of the European Parliament and of the Council<sup>36</sup>, irrespective of whether the transfer is executed via credit institutions or payment institutions or any other network used;
- (f) details of the wallet (including the nature or type of wallet, whether it is custodial or non-custodial), where the crypto-assets used or exchanged into official currency to acquire the holding were stored, of the crypto-asset service provider(s) used; and of the address identifiers of the originator and of the beneficiary on the DLT;
- (g) details of the DLT networks, architecture and protocols where the related smart contracts are deployed and the ledger transactions are performed and registered;
- (h) information on any financial arrangement with other persons who are or will be shareholders of the crypto-asset service provider.

For the purposes of point (d), where the lender is not a credit institution or a financial institution authorised to grant credit, the proposed acquirer shall provide comprehensive information and supporting evidence on the origin of the funds borrowed including, the lender's activity, legal form and place of residence, and any contractual clause empowering the lender to give instructions to the borrower about the qualifying holding.

2. Where the proposed acquirer is a trust, the method of financing the trust and resources ensuring the financial soundness of the trust to support the crypto-asset service provider.

---

<sup>36</sup> Regulation (EU) 2023/1113 of the European Parliament and of the Council<sup>36</sup> of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 9.6.2023, p. 1).

### *Article 9*

#### **Additional information for qualifying holdings of up to 20 %**

Where the proposed acquisition would result in the proposed acquirer holding a qualifying holding in the target entity of up to 20%, the proposed acquirer shall provide a document on the strategy to the competent authority of the target entity containing, where relevant, the following information:

- (a) the strategy of the proposed acquirer regarding the proposed acquisition, including the period for which the proposed acquirer intends to hold its shareholding after the proposed acquisition and any intention of the proposed acquirer to increase, reduce or maintain the level of his shareholding in the foreseeable future;
- (b) an indication of the intentions of the proposed acquirer towards the target entity, and in particular whether or not it intends to act as an active minority shareholder, and the rationale for that action;
- (c) information on the financial position of the proposed acquirer and its willingness to support the target entity with additional financial interests if needed for the development of its activities or in case of financial difficulties.

### *Article 10*

#### **Additional information for qualifying holdings of more than 20 % and up to 50%**

1. Where the proposed acquisition would result in the proposed acquirer holding a qualifying holding in the target entity of more than 20% and up to 50%, the proposed acquirer shall provide a document on the strategy to the competent authority of the target entity containing, where relevant, the following information:

- (a) all the information requested pursuant to Article 9;
- (b) details on the influence that the proposed acquirer intends to exercise on the financial position including dividend policy, the strategic development, and the allocation of resources of the target entity;

- (c) a description of the proposed acquirer's intentions and strategy towards the target entity, covering all the elements referred to in Article 11(2) with a level of detail proportionate to the influence in the target entity stemming from the acquisition;
2. By way of derogation from paragraph 1, depending on the structure of the shareholding of the target entity, the influence exercised by the shareholding of the proposed acquirer is considered to be equivalent to the influence exercised by shareholdings of more than 20% and up to 50%, the proposed acquirer shall provide the information set out in paragraph 1(a).

#### *Article 11*

#### **Additional information for qualifying holdings of more than 50%**

1. Where the proposed acquisition would result in the proposed acquirer holding a qualifying holding in the target entity of more than 50%, or the target entity becoming its subsidiary, the proposed acquirer shall provide a three year time horizon business plan to the competent authority of the target entity which shall comprise a strategic development plan, estimated financial statements of the target entity, and the impact of the acquisition on the corporate governance and general organisational structure of the target entity.
2. The strategic development plan referred to in paragraph 1 shall indicate, in general terms, the main goals of the proposed acquisition and the main ways for achieving them, including:
- (a) the overall aim of the proposed acquisition;
  - (b) financial goals which may be stated in terms of return on equity, cost-benefit ratio, earnings per share, or in other terms as appropriate;
  - (c) the possible redirection of activities, products, targeted customers and the possible reallocation of funds or resources expected to impact on the target entity;
  - (d) general processes for including and integrating the target entity in the group structure of the proposed acquirer, including a description of the main interactions to be pursued with other companies in the group, as well as a description of the policies governing intra-group relations.

With regard to point (d), for proposed acquirers authorised and supervised in the Union, information about the particular departments within the group structure which are affected by the transaction shall be sufficient.

3. The estimated financial statements of the target entity referred to in paragraph 1 shall, on both an individual and, where applicable, a consolidated basis, for a period of three years, include the following:

- (a) a forecast balance sheet and income statement;
- (b) forecast prudential capital requirements and reserve of assets;
- (c) information on forecasted level of risk exposures including market, operational (such as cyber and fraud), credit and environmental risks as well as other relevant risks;
- (d) a forecast of provisional intra-group transactions.

4. The impact of the acquisition on the corporate governance and general organisational structure of the target entity referred to in paragraph 1 shall include the impact on:

- (a) the composition and duties of the members of the management body, and where applicable the main committees created by such decision-taking body including information concerning the persons who will be appointed as members of the management body;
- (b) administrative and accounting procedures and internal controls, including changes in procedures and systems relating to accounting, internal audit, compliance including anti-money laundering and counter terrorism financing, and risk management, and including the appointment of the key functions holders of internal audit, compliance officers and risk managers;
- (c) the overall ICT and technology architecture including any changes concerning the policy relating to ICT third-party service providers of critical or important functions referred to in Article 28(2) of Regulation (EU) 2022/2554<sup>37</sup>, the data flowchart, the in-house and external software used and the essential data and systems security procedures and tools including back-up, business continuity plans and audit trails;
- (d) the policies governing third-party service providers of critical or important functions, including information on the areas concerned, on the selection of service providers, and on the respective rights and obligations of the principal parties as set out in contracts such as audit arrangements and arrangements for the custody and investment of the reserve of assets, and the quality of service expected from the provider;

---

<sup>37</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).

- (e) any other relevant information pertaining to the impact of the acquisition on the corporate governance and general organisational structure of the target entity, including any modification regarding the voting rights of the shareholders.

## *Article 12*

### **Reduced information requirements**

1. Where the proposed acquirer has been assessed for the acquisition or increase in qualifying holdings by the same competent authority of the target entity in accordance with Articles 41(1) or 83(1) of Regulation (EU) 2023/1114, Article 13 of Directive 2014/65/EU of the European Parliament and of the Council<sup>38</sup>, Article 23 of Directive 2013/36/EU of the European Parliament and of the Council<sup>39</sup>, Article 59 of Directive 2009/138/EC of the European Parliament and of the Council<sup>40</sup>, Article 32 of Regulation (EU) No 648/2012 of the European Parliament and of the Council<sup>41</sup>, within the previous two years from the submission of the notification, such proposed acquirer shall only submit to the competent authority of the target entity the information that is specific to this proposed acquisition or that has changed since the previous assessment.

The proposed acquirer shall submit a signed declaration indicating the exact information set out in this Regulation that has not been submitted, certifying that it has not changed since the previous assessment and that it is still true, accurate and up-to-date.

2. Without prejudice to paragraph 1, where the proposed acquirer is an undertaking authorised by and subject to the ongoing prudential supervision of the same competent authority of the target entity, it shall only submit the information set out in this Regulation specific to the proposed acquisition and shall be exempted from the submission of the information already in possession of that competent authority.

The proposed acquirer shall submit a signed declaration indicating the exact information referred to in this Regulation that has not been submitted because already in possession of that competent authority and certifying that such information is true, accurate and up-to-date.

---

<sup>38</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 (OJ L 173, 12.6.2014, p. 349).

<sup>39</sup> Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

<sup>40</sup> Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335 17.12.2009, p. 1).

<sup>41</sup> Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201 27.7.2012, p. 1).

3. For purposes of this Article, information specific to the proposed acquisition set out in this Regulation includes at least all of the following:

(a) where the proposed acquirer is a natural person:

- (i) information set out in Article 1(1);
- (ii) information set out in Article 2, points (c) to (i) where the proposed acquisition is covered by paragraph 1, information set out in Article 2, points (f) to (i) in case of proposed acquisitions covered by paragraph 2;
- (iii) information set out in Article 5,
- (iv) information set out in Article 6,
- (v) information set out in Article 8;
- (vi) the information set out in Article 9, 10 or 11, as applicable.

(b) where the proposed acquirer is a legal person, a trust, an alternative investment fund (AIF) in accordance with Article 4(1)(a) of Directive 2011/61/EU or an undertaking for collective investment in transferable securities (UCITS) in accordance with Article 1(2) of Directive 2009/65/EC, or a sovereign wealth fund:

- (i) information set out in Article 1(2), points (a) to (f);
- (ii) information set out in Article 3(1), points (a) (ii) to (iv), as well as points (b) to (d), and in Articles 5 as applicable, where the proposed acquisition is covered by paragraph (1) of this Article, also information set out in Article 3(1), point (i), points (i) to (iv);
- (iii) Information set out in Articles 6 and 7;
- (iv) information set out in Article 8;
- (v) the information set out in Articles 9, 10 or 11, as applicable.

### *Article 13*

#### **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