MiCA HANDBOOK

FOR CRYPTO-ASSET SERVICE PROVIDERS

Contents

Introduction

This Handbook explains in plain language the requirements for crypto-asset service providers (CASP) under Regulation (EU) 2023/1114 (MiCA), and all related regulatory products that complete MiCA regulation.

All main applicable requirements are outlined in this single document, and brief guidance on how to implement those requirements in a practical perspective is also provided. This will support CASPs when navigating the European Union's (EU) regulatory framework, and contribute to the journey of understanding MiCA.

The Handbook is distributed free of charge. The information provided in this Handbook is for general information purposes only.

1. List of legal acts

The framework for regulation of crypto-asset in the EU, consists not only of MiCA regulation, but is also covered by a series of Regulatory Technical Standards (RTS) and Guidelines (GL), together called Level 2 and 3 regulatory products, which complete MiCA regulation and are mandatory for CASPs to comply with. The Table below provides a list of all Level 2 and 3 regulatory products that are relevant for CASPs.

Reference to MiCA article	Type*	Link to legal act**
AUTHORIZATION		
Article 62(5)	RTS	RTS on authorisation of crypto-asset service providers
Article 62(6)	ITS	ITS on authorisation of crypto-asset service providers
GOVERNANCE		
Article 18(2); 62(2)(j or h)	GL	Joint Guidelines on the suitability assessment of HQ shareholders ((EBA/GL/2024/09, ESMA75-453128700-10)
Article 21(3); 63(11)	GL	Joint Guidelines on the suitability of member of the management body (EBA/GL/2024/09, ESMA75-453128700-10)
Article 72(5)	RTS	RTS on conflicts of interest for crypto-asset service providers
Article 84(4)	RTS	RTS on the assessment of proposed acquisition of HQ of CASP
OPERATIONAL REQUIREMENTS		
Article 2(5)	GL	Guidelines on the conditions and criteria for the qualification of crypto-asset as financial instruments
Article 6(11), 19(10), 51(10)	ITS	ITS on standard forms and templates for the crypto-asset white paper
Article 14(1)(d)	GL	Guidelines on the maintenance of systems and security access protocols in conformity with appropriate Union standards
Article 66(6)	RTS	RTS on content, methodologies and presentation of sustainability indicators on adverse impacts on the climate and the environment
Article 68(9;10)	RTS	RTS on record-keeping by crypto-asset service providers
Article 68(10)	RTS	RTS on measures that crypto-asset service providers must take to ensure continuity and regularity in the performance of services
Article 71(5)	RTS	RTS on complaints handling by crypto-asset service providers

Article 76(16)(a)	RTS	RTS on trade transparency
Article 76(16)(b)	RTS	RTS on content and format of order book records
Article 109(8)	RTS	RTS on the data necessary for the classification of white papers
MARKET ABUSE		
Article 88(4)	ITS	ITS on technical means for appropriate public disclosure of inside information
Article 92(2)	RTS	RTS on arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-asset
SERVICE SPECIFIC		
Article 81(14)	GL	Guidelines on certain aspects of the suitability requirements and format of the periodic statement for portfolio management activities under MiCA
Article 82(2)	GL	Guidelines on the procedures and policies, including the rights of clients, in the context of transfer services for crypto-asset
SUPERVISION		
Article 61(3)	GL	On the draft guidelines on reverse solicitation under the Markets in Crypto-asset Regulation (MiCA)
Article 95(10)	RTS	RTS on NCA cooperation

**RTS (Regulatory Technical Standards) means a complementary regulation that is mandatory without national transposition. ITS (Implementing Technical Standards) has the same status as the RTS, but the purpose of an ITS is to provide technical details (i.e. to outline reporting templates, white paper templates, etc). GL (Guidelines) are not mandatory, and are subject to the transposition or other actions by a national competent authority (NCA) (i.e. an NCA can decide not to comply with Guidelines, or to transpose them to national legal acts).*

EU agencies (ESMA, EBA) are granted a mandate in the main regulation to develop drafts for these regulatory products (RTS, ITS, GL). The mandate already contains what shall be included in the drafts for RTS/ITS/GL, therefore ESMA/EBA cannot deviate from the mandate when developing the regulatory products. In exceptional cases regulatory products can be drafted by the initiative of the agencies. Once developed the draft RTS/ITS shall be adopted by the European Commission (EC), so may change even after the ESMA/EBA Final Report. Guidelines have been adopted by ESMA/EBA, therefore are not required to be submitted to the EC for adoption after final version.

***as of December 2024 the European Commission has not adopted RTS, only a draft RTS is available in the ESMA Final Report. Therefore RTS may still change subject to EC adoption. Guidelines have to be adopted by ESMA/EBA, therefore they should be the same as in the Final Report.*

Abbreviations used in this Handbook

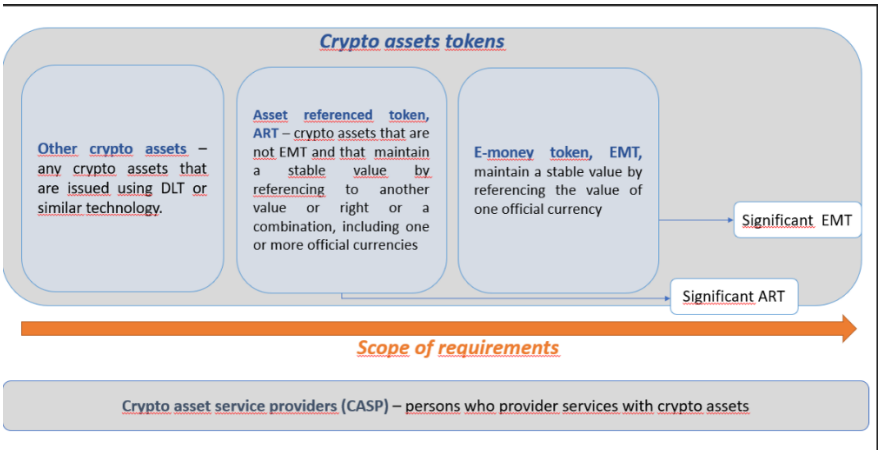
Abbreviation	Definition
CET1	Common Equity Tier 1
EC	European Commission
EU	European Union
ITS	Implementing Technical Standards
MiCA	Regulation (EU) 2023/1114 on markets in crypto-asset
MS	Member State
NCA	National Competent Authority
RTS	Regulatory Technical Standards

2. Scope of MiCA

Article 2, Article 4(3) of MiCA

Regulation (EU) 2023/1114 (MiCA) applies to crypto-asset that are issued using distributed ledger technology (DLT) or, to encompass technology that may emerge in the future, similar technology. Instead of regulating the crypto-asset itself, MiCA sets requirements for the provision of services by crypto-asset service providers (CASPs), and for the public offering of crypto-asset. This is because regulation is enforceable only by setting requirements to persons (legal entities) rather than assets.

All crypto-asset fall under MiCA by use of an all-encompassing definition of a crypto-asset. There are three types of crypto-asset (tokens): i) asset-referenced tokens (ART), ii) e-money tokens (EMT) these two are so-called stablecoins, and the third type is for other crypto-asset, which encompasses every crypto-asset except ART and EMT. The scope of requirements depend on the rights that the issuer is obliged to grant to token holders under MiCA. Issuers of ART and EMT must redeem tokens either at market (ART) or par (EMT) value, so they are regulated strictly. There are significant ARTs and EMTs that are subject to even more requirements. Issuers of other crypto-asset are not obliged to grant any rights, except the ones which they write down in a white paper (technically, they can promise anything they wish), so they are regulated more lightly.



Scope of MiCA requirements by type of crypto-asset

Even if all crypto-asset should fall under the scope of MiCA, this regulation is drafted in such a way that certain crypto-asset are excluded explicitly from its scope, either totally or partially (only from some of requirements).

What is excluded totally:

- Crypto-asset which according to their features qualify as financial instruments, deposits, insurance products or similar instruments that are already regulated by the EU capital markets framework. These are indeed tokenized instruments. For example financial instruments (common shares, derivatives, and other) are regulated by the MiFID II framework, so MiFID II rules will continue to apply for those instruments in tokenized. The same applies to deposits, pension products, etc. The idea is to maintain technological neutrality. However, this principle is not maintained for e-money tokens (EMT). EMTs will

be subject to the E-money directive and MiCA requirements. It was decided to apply MiCA to them in order to provide holders of EMTs with transparency disclosure (white paper).

- Crypto-asset that are unique and not fungible with other crypto-asset such as NFTs, loyalty schemes and similar. They are not negotiated - capable of being traded - on the capital markets, so there is no need to apply MiCA for them. However the substance of the instrument should be assessed, as there are NFTs in the market that could potentially fall under the scope of MiCA requirements.

For the above mentioned crypto-asset, neither requirements for the provision of crypto-asset services apply, nor requirements for the public offering. Issuers can offer them in the EU without applying MiCA rules.

Further, there are a group of crypto-asset that are excluded from only the public offering requirements, but the requirements for the provision of crypto-asset services may apply. These are as follows:

- Small issuances (offered to less than 150 persons, or offer does not exceed 1 million euro during 12 month or offered to qualified investors) are exempted from the requirement to prepare white paper and marketing communication requirements (MiCA Article 4(2)). But CASPs should comply with MiCA when providing crypto-asset services with them.
- Crypto-asset are offered for free, utility tokens for the purpose of usage in a limited network, tokens that are created during the mining process (MiCA Article 4(3)). In such case the requirements for the provision of services (in particular for the provision of custody and administration of crypto-asset on behalf of clients, or for providing transfer services for crypto-asset) does not apply if the crypto-asset are not admitted to a trading platform. If CASPs provide other than those two services with crypto-asset mentioned in this paragraph, then they should comply with MiCA when providing crypto-asset services.

The definition of public offer is vague and is not always straightforward. Furthermore, under MiCA it is admitted that other persons could offer crypto-asset in the EU and those persons are subject to MiCA requirements instead of issuers. This is the case where crypto-asset have no identified issuer, in which case Article 5 instead of 4 of MiCA applies to a person that offers, or admits to trading, such crypto-asset. However, since public offering is more relevant to issuers, it will not be covered further in this Handbook.

What is relevant for CASPs is the provision of crypto-asset services. Even for crypto-asset that have no identified issuer, a CASP should always be identified when providing services with such crypto-asset. Crypto-asset services are listed in Article 3(1)(16) of MiCA, and when someone provides those services professionally for others an authorization as a crypto-asset service provider is required. Therefore crypto-asset services to be considered under MiCA, are as following:

- Custody and administration of crypto-asset on behalf of clients (Article 3(1)(16)(a)). This means safeguarding (including controlling) of crypto-asset on behalf of clients.
- Operation of a trading platform for crypto-asset (Article 3(1)(16)(b)). This is the operation of a trading venue where clients can exchange their interests (regarding price, volume) of

buying/selling crypto-asset, and trading venues that bring together their interests. In a conventional market it would be a stock exchange, MTF, OTF.

- Exchange of crypto-asset for funds or other crypto-asset (Article 3(1)(16)(c and d)). This service is crypto unique. This service is like currency exchange in conventional markets.
- Execution of orders for crypto-asset on behalf of clients (Article 3(1)(16)(e)). This is a conclusion of buy/sell transactions. CASPs should assess if they provide this service in combination with other services.
- Placing of crypto-asset (Article 3(1)(16)(f)). This is the marketing of crypto-asset on behalf of an issuer or offeror.
- Reception and transmission of orders for crypto-asset on behalf of clients; (Article 3(1)(16)(g)). Clients' orders are received and then transmitted (both of those) to other service providers for the execution of order.
- Providing advice on crypto-asset (Article 3(1)(16)(h)). Advice is a recommendation to buy, sell, hold, or perform other actions with crypto-asset. It shall be provided to the concrete client in his/her financial and non-financial (such as ability to bear risk) capability.
- Providing portfolio management on crypto-asset (Article 3(1)(16)(i)). This is a service where a portfolio manager (or other persons) manages portfolios of crypto-asset for other persons under pre-defined mandates.
- Providing transfer services for crypto-asset on behalf of clients (Article 3(1)(16)(j)). This means the transfer (move) of crypto-asset from one's DLT address or account to another. Usually this service is provided in combination with other services.

This list is exhaustive. So other services, such as crypto-asset lending and staking activities are not included in this list. Therefore, such services, not included in the list above, are not considered as crypto-asset (regulated) services at the current time, and so do not currently need to be authorized to provide such services. Another example is dealing on one's own account activity. If this would be considered a crypto-asset service, then every private person who buys and sells crypto-asset for the intention to gain profits would be subject to MiCA. However, as of writing there is a pending ESMA Q&A on this, so it may be interpreted by EC' differently.

Crypto-asset services can be provided only by two types of persons:

- CASPs authorized under MiCA, this will apply to new types of financial institutions, and
- existing financial institutions, such as a credit institution, central securities depository, investment firm, market operator, electronic money institution, UCITS management company, or an alternative investment fund manager that can provide certain crypto-asset services based on their existing license for traditional services.

Existing financial institutions do not need new authorization. Instead they are required to apply for an extension of their authorization, by providing their national competent authority (NCA) notification, with certain documents, 40 days before the provision of such services. In fact, under MiCA there is almost no chance that an existing financial institution will be prohibited to provide crypto-asset services.

Meanwhile CASPs operating as new institutions, will need to be fully authorized to provide MiCA crypto-asset services. In order to receive a license and to comply with MiCA (and to keep a license), the CASP will need to fully implement MiCA requirements. In the following sections this Handbook will explain the MiCA requirements thoroughly.

3. Governance requirements

Article 68 MiCA, Article 69 MiCA

Crypto-asset service providers shall have a registered office in a Member State where they carry out at least part of their crypto-asset services, and at least one of the directors shall be resident in the Union.

MiCA also sets requirements for the management body, and for the shareholders of qualifying holdings of a CASP. The management body shall be understood as an executive management body (Management Board) and a non-executive management body (Supervisory Board). The structure of the management body if dual or unitary, differs among EU MS. Meanwhile a qualifying holding is where a shareholder directly or indirectly acquires more than 10 per cent of the capital or of the voting rights of a CASP.

For authorization, the following shall be provided to the NCA:

- Suitability Assessment Policy,
- Assessment of each member of the management body (i.e. a report/questionnaire and relevant documents proving the assessment),
- Assessment of collective suitability (i.e. a report/questionnaire),
- Documents of shareholders of qualifying holding provided to the NCA for their assessment.

3. 1. Assessment of management body

Article 68 MiCA

Under Article 68(1) of MiCA, members of the management body shall be of sufficiently good repute, and possess the appropriate knowledge, skills and experience, both individually and collectively, to perform their duties (so called suitability assessment). In addition, further details are specified in Joint ESMA/EBA Guidelines on suitability of the management body. Which is to say, only a person who is assessed as suitable by a CASP and an NCA can be appointed as a member of management body. Therefore the CASP shall assess if a person:

- possesses good reputation,
- possesses relevant knowledge, skills and experience to manage a CASP,
- is able to devote sufficient time for its functions.

A member shall be suitable at all times. It means that if some factors show that a member may not be suitable anymore, a CASP should take actions (for example to replace that member).

In general, if a member is not suitable because of his or her reputation, then a CASP cannot appoint that person. Assessment of reputation is based on the element of proof. In other words, if there are no reasons to suspect that a person's reputation is not good, then such person is considered as suitable. From a practical perspective the process for the assessment of reputation is quite simple. A member shall provide a CASP with an official certificate from the authority where the member is a resident.

If a person does not possess the suitable knowledge, skills, or reputation, such person can be appointed, but in such cases the CASP should be able to provide suitable reasoning why it considers that person as a suitable person.

Collective suitability should also be assessed. Collective suitability means that all appointed members shall collectively combine their knowledge, skills, and experience, in order to ensure sound management of the CASP.

Assessment processes of individual and collective suitability should be defined by the Suitability Assessment Policy. The policy could include principles of the selection, monitoring and succession planning of its members, and for re-appointing existing members, and should set out at least the following:

- The process for how a CASP selects members and assesses suitability,
- Criteria used for the assessment. Those criteria in general, can be taken from ESMA/EBA guidelines of suitability assessment, in particular the Annex that provides the template,
- Criteria for collective suitability. This also can be taken from the Annex of the guidelines.
- Diversity aspects,
- Documentation and retention provisions.

In summary, the process in general, should reflect the following:

- A CASP shall establish a Suitability Assessment Policy,
- According to the process defined in the Policy the CASP assessed suitability in two cases – when a new member is appointed, and when re-assessment is performed. Re-assessment can be carried out either when a CASP has become aware of circumstances which could have an impact for the CASP, or on an annual basis. Re-assessment also should be carried out when the business model, or the activity of the CASP is changing significantly. Sufficient time commitment should be assessed if a new position is taken (external or internal).
- Each CASP shall inform their NCA about the assessment, and provide the required documents (Article 69 of MICA). In general, a member of the management body cannot take a position if the NCA has not approved it.

Regarding sufficient time commitment, chair of the management body shall be independent (expect when a CASP is in a group and chair takes a role in parent company). Members of executive board should devote at least half of their time to a CASP (which means 0.5 FTE). CEO should devote 100 % FTE (1 FTE)

Besides requirements for the members of management body, there is also a requirement of Article 68(5) of MiCA, that employees should have the knowledge, skills and expertise necessary to perform their functions. However, there is no requirement to assess formally (i.e. by preparing a report of their suitability) employees' suitability for a position.

3.2. Assessment of the shareholders of qualifying holding

Aritlce 68 of MiCA, Article 82, 84 of MiCA

Shareholders of qualifying holding (whose shares in the company exceed 10 %) must possess good reputation. Good reputation shall be understood as no previous or ongoing criminal conviction of AML/TF and other criminal or other convictions.

The assessment of such shareholders is carried out by the NCA according to the procedure set out in ESMA/EBA Guidelines, on the assessment of the suitability of the shareholder. This is standard procedure for other regulated entities as well. Additionally, if the funds to establish a company (i.e. a CASP) are acquired via crypto-asset, the NCA will check the information regarding such funds (DLT address, crypto-asset account number, a unique transaction identifier).

Every shareholder must inform the NCA if their holding of shares exceed certain share. They must inform NCA in the following cases:

- Where a person, or acting in concert with other persons, decide to acquire a share of qualifying holdings that reach or exceed 20 %, 30 %, or 50 %, the person shall get prior approval from NCA.
- Where a person disposes or reduces their qualifying holding that would result in a fall below 10 %, 20 %, 30 % or 50 %, that person shall inform the NCA in advance and indicate the size of disposable holdings.

The NCA has 60 working days to make an assessment of the acquisition, however, they can request additional documents, and pause the assessment for 20 working days (30 days where a person is not EU resident).

The assessment takes into account good reputation and financial soundness of a person. All criteria and required documents are specified in ESMA's RTS on the assessment of the proposed acquisition.

4. Prudential requirements

Article 67 of MiCA, Article 3 of RTS on authorization

To comply with own funds requirements a CASP shall calculate the required amount of own funds (as explained in section 4.1) and then at all times hold own funds in a form of eligible instruments (as explained in section 4.2). From a practical perspective it is not enough to have only the minimum amount of own funds. Usually the NCA require a CASP to hold a much higher amount, in order to cover additional risk, and during the first years of activity a company may generate loss.

In addition, CASPs must monitor own funds at all times (Article 3 of RTS on authorization). In order to monitor own funds at all times, a CASP should have a written internal procedure, and be able to prepare periodic reports, or have a suitable system that will allow to do that. Monitoring could be understood as a regular follow-up process to ensure that a CASP complies with own funds requirements constantly. Periodic (i.e. monthly) internal reports templates can be the same as for an investment firm (adapted to CASP requirements), and submitted for the management body to review and approve.

4.1. Own funds requirement

A CASP shall have at all times own funds that are the higher of one of those:

- Permanent minimum capital (in other words, initial capital), or
- Fixed overheads requirement.

Permanent minimum capital is the initial capital that is specified in the regulation, and it's amount is fixed. Meanwhile own funds, is capital that must be maintained at all times when a company is operational.

The amount of permanent minimum capital required for CASPs depends on the services they provide. Annex IV specifies an amount of initial capital for all services. Riskier activity requires more capital. For example, the operation of trading platform is riskier, because a CASP is subject to more operational risk. For the operation of a trading platform, initial capital is 150 000 euro, for crypto-asset exchange services, and for the provision of custody service, initial capital is 125 000 euro, for all other services the amount is 50 000 euro.

Fixed overheads requirement (FOR) can be understood as one quarter of the previous year's expenses, taken from previous year's financial statements. Financial statements shall be either audited or, either approved by national supervisors (which is not common practice in the market, so this is unlikely). The exact formula is as follows:

FOR = (previous year's fixed overheads – deductions allowed under Article 67(3) of MiCA)) ÷ 4

The previous year's fixed overheads shall be taken from applicable accounting standards. Applicable accounting standards are typically classed as recognized accounting standards that are in standard usage, so in this case it should be either national accounting standards or IFRS depending what a CASP uses.

Deductions are overheads that are discretionary by the company. This can include staff bonuses, employees', directors' and partners' shares in profits, other appropriations of profits and other variable remuneration, non-recurring expenses from non-ordinary activities. The last item shall be not related with the main activity of the company, and should not be frequent.

The fixed overheads requirement stays the same during one financial year (since overheads are from the previous year). It must then be recalculated annually (because the overheads amount for the next year will be different).

If a company is newly established and has not been in operations during the previous year, then the fixed overheads requirement is calculated by taking into account the projections in the business plan. Therefore the projections should be accurate and realistic.

For example, if a CASP provides custody service, portfolio management services and operates a trading platform, its permanent minimum capital shall be 150 000 euro. If a CASP has calculated that its fixed overheads requirement is 500 000 euro, then the amount of own funds requirement is 500 000 euro. And that amount should be covered in instruments as it is explained in the next section.

4.2. Own funds instruments

When the own funds requirement is calculated, a CASP has two options for how they choose to cover that amount:

- by Common Equity Tier 1 (CET1) capital instruments, or
- by insurance policy.

Using an insurance policy is likely not to be the most used option. Any insurance policy for this purpose, must comply with requirements under Article 67(5) and 67(6) of MiCA, such as requirements for the duration (i. e. no less than one year), the cancellation is possible only after 90 days' notice period, the policy shall be disclosed on the company website, and must include insurance against risks listed in Article 67(6) of MiCA.

The other option is to cover the required own funds amount by using CET1 instruments (that is the highest quality of regulatory capital and instruments are such as equity and retained earnings). CET1 instruments are items that are listed in Articles 26 to 30 of Regulation (EU) No 575/2013 (CRR). In general CET1 instruments are common shares of the company, share premiums, retained earnings, accumulated other comprehensive income, or other reserves. However, all such instruments must comply with criteria that are specified in relevant CRR articles. If an instrument does not comply with the necessary criteria, it cannot be considered as CET1 instrument, and so cannot be used. Illiquid items or items that can't be valued shall be further deducted from CET1 capital. Deductions are specified in Article 36 of CRR, but exemptions on threshold under Articles 46 and 48 of CRR shall not be applied.

In summary, the own funds requirement for a CASP is relatively simple compared to other regulated financial service entities. Such entities are usually subject not only to the own funds requirement, but also to so called Pillar 2 requirements. Pillar 2 requirements are additional capital requirements in addition to minimum requirements. They consist of internal capital and liquid asset assessment processes (so called ICAAP and ILAAP), where a company must calculate additional own funds requirements, by the level of risk associated to it and its activity. The NCA then, on regular basis, performs a supervisory review and evaluation process (SREP) which assesses if ICAAP and ILAAP sufficiently cover the risks. At the current time, MiCA have not set Pillar 2 requirements for CASPs. However, there may be national requirements, so each CASP should check national regulation.

If own funds become lower than the requirement, then the CASP could inform its NCA and provide a plan how own funds will be restored. Otherwise it may be considered as a serious breach of regulatory requirements.

4.3. Documents for the authorization

Full list of documents in relation to own funds:

- A description of the applicant's prudential safeguards in accordance with Article 67 of MiCA.
- Authorization requires the provision of suitable forecasts for the next 3 business years. The forecasts shall be made both for normal and stressed scenarios, and should include assumptions, expected number and type of clients, volume of orders and transactions,

and the expected maximum amount of crypto-asset under custody. Generally the forecasts should demonstrate that the CASP will have robust capital, and the own funds requirement will not fall under the minimum ratio.
- Financial statements for the last three years (if a company is already established), and if an audit has been performed, then audited statements should be provided.
- The description of own funds planning and monitoring procedure.
- Proof that the CASP has necessary own funds. For established companies this will mean financial statements. For new companies, a bank statement showing the amount may be used.
- If an insurance policy is used, then the information of the insurance provider and a copy of the policy and agreement is required.

5. Conflict of interest prevention, management and disclosure

Aritcle 72 of MiCA, RTS on Conflict of interest

A CASP shall identify, prevent, manage and disclose conflicts of interest between the CASP and its shareholders, management body, employees, and clients, and between two or more clients whose mutual interests may conflict. The scope is wider compared to MiFID, which does not include conflict of interests between shareholders.

A conflict of interest can essentially cover any activity which leads to a financial gain (or other kind), acting in favor of own (or of connected persons, other clients) interests, instead of providing services in the best interests of the client. This may cause damage to the interests of one or more clients. In other word it is the provision of services in such a way where a client is in worse (financial) position.

If a conflict of interest can be managed, then the CASP should disclose it to the client (if the client is willing to accept that situation, then those services can still be provided). However, if conflict of interest cannot be managed appropriately, then the CASP should prevent it (i.e. or do not provide relevant services to a client).

Requirements for conflict of interest management include a subset of arrangements that a CASP should implement:

- Conflict of interest management and disclosure,
- Remuneration management,
- Personal account dealing management.

5.1. Conflict of interest management and disclosure

In order to manage conflict of interest requirements under MiCA, a CASP shall:

- Establish a Conflict of Interest Policy and review it annually. This policy in general should provide an outline of the appropriate conflict of interest management procedure. The policy should include a description of conflict of interest cases, specify measures to identify, prevent, manage and disclose such conflicts, and give a clear reference to the organisational and managerial structure of the CASP.

- Make a disclosure on its website, of the general nature and sources of conflict of interest, and what actions are taken to mitigate them. The disclosure shall include the role and capacity in which the crypto-asset service provider is acting when providing the crypto-asset service to the client, the nature of the conflict of interest, the associated risks, and the steps and measures taken to prevent or mitigate the identified conflicts of interest. The appropriate disclosure shall be made in languages used by crypto-asset service providers to market their services and communicate with their clients.
- Establish a register of conflict of interest situations and maintain it. The register shall cover concrete cases and include decisions taken.
- Where a CASP is a part of the group, it shall take additional measures as specified in Article 4(2) of the RTS.
- Inform employees about the conflict of interest procedure, and organize suitable regular training for them.
- There are additional requirements where a CASP provides placing services to ensure that the CASP acts in the best interest of this client. If a CASP at the same time also offers pricing services, execution of orders, research services, or where the placing service is provided for itself or an entity in the group, the CASP shall ensure that the pricing does not raise a conflict of interest. To avoid such a situation, the CASP shall keep a registry of placing operations.

5.2. Remuneration requirements

MiCA does not regulate the remuneration of CASP employees directly. However, Article 5 of the RTS on conflict of interest specifies certain rules for the CASP's remuneration. The main purpose of it is to manage conflict of interests by implementing rules for remuneration. Such requirements apply to employees of a CASP, members of the supervisory and management bodies, other persons for whom a CASP has direct responsibility for, or those who are involved in the provision of CASP services under an outsourcing arrangement (such as external employees, agents). Regarding the employees, the requirements apply to those employees that have an impact on services (for example sales persons, portfolio manager, investment directors) or are responsible for corporate decisions (for example senior management) and where remuneration or other benefits/payments could create a conflict of interest. Those are situations which could lead employees to act in favor of themselves instead of clients or the CASP. Remuneration of such persons should thus comply with the requirements, and other qualitative criteria of the RTS on conflict of interest.

In order to implement remuneration requirements a CASP shall:

- Prepare a Remuneration Policy,
- Set a ration or criteria regarding fixed and variable remuneration for certain types of employees (that are mentioned in a paragraph above),
- A CASP shall document remuneration policy and practice.

There is no requirement to set a ratio between fixed and variable remuneration for such persons, however RTS requires that fixed and variable components shall be maintained. In practice it means that fixed remuneration should make up a larger part of total remuneration. Where variable remuneration is paid, then before awarding it a CASP should take into account not only

quantitative criteria (i. e. volume of sales) but also assess qualitative criteria (i.e. number of complaints received against this employee, ethical behavior).

The requirements shall be based on the proportionality principle. Small CASPs can implement this requirement by applying the minimum arrangements. However larger CASPs should take more robust measures.

5.3. Personal transactions

Personal account dealing requirements will affect the positions of crypto-asset that certain persons (i.e. managers, shareholders, employees) hold on their own accounts. This is because such persons won't be able to hold certain crypto-asset positions, where a conflict of interest may arise.

MiCA and RTS on conflict of interest, states that connected persons (shareholders, members of management body, employees) cannot enter into transactions that breach market abuse requirements, misuse information, or make improper disclosure of confidential information where it conflicts or is likely to conflict with the obligations of the CASP.

CASPs shall inform connected persons about the restrictions on personal account dealing. Then connected persons shall inform the CASP of any relevant personal transactions of connected persons. This information can be provided in a form of notification or other procedures enabling the crypto-asset service provider to identify such transactions. The CASP shall keep records of such notified personal transactions, including the ones identified by the CASP itself, and the decision taken.

In order to implement personal transaction requirements a CASP shall:

- Prohibit personal account dealing for certain employees and under certain circumstances (for example where a person possesses inside information).
- Maintain lists of prohibited crypto-asset for personal account dealing, and of persons who posses inside information, or crypto-asset where a conflict of interest exists.
- The CASP shall appoint a suitable employee who can collect the relevant information about employees and members of the management body, with regard to personal account dealing.
- Provide suitable training on personal account dealing to employees and members of the management body.

Personal transactions include any transactions or positions of crypto-asset, where the person acts in the scope of personal capacity. The requirements apply to connected persons and their family members, or a person with whom there is a close relationship (spouse or partner, a dependent child or stepchild, a family member who has shared the same household as that person for at least one year on the date of the personal transaction concerned or the previous 5 years), or a person in respect of whom the connected person has a direct or indirect material interest in the outcome of the transaction, other than obtaining a fee or commission for the execution of the transaction.

6. Complaints handling

Article 71 MiCA, RTS on complaints handling

Crypto-asset service providers shall accept complaints from clients and implement procedures for the acceptance and handling (investigation) of such complaints. Complaint means a statement of dissatisfaction addressed to a CASP by one of its clients relating to the provision of one or more crypto-asset services. So only complaints that are related to MiCA services are in the scope of such requirements (for example if a client complains about the price volatility of a crypto-asset, then such complaints could be out of scope).

All clients shall be able to submit a complaint free of charge. CASPs shall be able to admit complaints in a paper or/and electronic form. Confirmed methods for how clients can submit complaints (for example by email, at the office) shall be specified in the Complaint Handling Procedure. There is no need to accept complaints via social media, unless the CASP itself has specified that in the Procedure and it is willing to accept such complaints.

A CASP shall facilitate the clients' right to complain. This facilitation is achieved by establishing a specific procedure for that, and the CASP must:

- Draft a Complaints Handling Procedure. The procedure shall contain information set out in Article 1(2) of the RTS complaints handling.
- Prepare a summary (containing only the main information) of the Complaints Handling Procedure, and publish it on the company website together with the template of Complaint, which is set out in Annex I of RTS. A summary and templates shall be published in all languages used by the crypto-asset service provider to market its services or communicate with clients.
- Maintain a registry of complaints (in any form, example could be Excel table) that records all complaints and details.
- Immediately after the reception of a complaint, inform the client if the complaint is admissible.
- Provide a client confirmation of the acknowledgment of the complaint, and explanation if the investigation exceeds the specified timeline. Acknowledgement shall contain all details that are required by Article 4(3) of RTS on Complaints Handling.
- Implement procedure for monitoring and analysis of received complaints. Analysis shall include the average processing time, the number of complaints received, the categories of the topics to which complaints relate, outcomes of investigations. For example analysis could be quarterly report by the person in charge of complaints management.
- A person in charge of complaints shall provide a report to the management body, including analysis and measures taken to restore deficiencies.

The CASP shall investigate the complaint and provide a decision within 2 months after receipt of the complaint. There may be exceptional cases that involve more complicated complaints, and in such cases the CASP may provide a final decision which exceeds 2 months, but if this occurs, the CASP must regularly update the client and provide reasons why the investigation took longer than usual.

A CASP shall accept complaints in all languages used by the CASP. The CASP shall admit complaints in any language used by a CASP to market its services or communicate with clients, and in official languages of where the CASP is authorized, and all host member states.

7. Outsourcing

Article 73 of MiCA

Under outsourcing arrangements a CASP can delegate some of its activities or functions to other persons/entities where another entity performs a process, a service, or an activity that a CASP would perform itself. As an example this could be sales/distribution activities. MiCA does not have a tied agent regime, however, their functions can be delegated by outsourcing. Where a CASP outsources its services or activities to other entities the CASP remains responsible for the requirements under MiCA. Additional requirements also apply for outsourcing. Additional requirements for outsourcing are the following:

- The CASP shall assess the quality of persons/entities for whom they outsource functions. The CASP could define core (significant) functions and services and apply more stringent arrangements for them.
- Ensure that written agreements are signed, and that those agreements include suitable data protection provisions, specify their rights and obligations, and include the right for a CASP to terminate the agreement.
- Establish a Policy on outsourcing that includes contingency plans and exit strategies – a strategy for how to exit the agreement if a CASP would no longer use or be able to use the outsourced entity.
- The CASP shall monitor the outsourced services and have direct access to the relevant information of the outsourced services.
- The CASP shall ensure that if an NCA requests supervision information it will be accessible, including the ability to allow onsite inspection (investigation at the premises). This could be done by relevant provisions in the agreement.

8. Market abuse requirements

Title VI of MiCA, RTS on market abuse

Market abuse requirements set rules for fair trading of crypto-asset. Those requirements limit unfair practices such as artificial price influence, front running, wash trading, spoofing, or similar practices. If any person (even not subject to other titles of MICA) engages into such behavior that person is subject to severe penalties and/or other supervisory actions. Even if it is very hard to catch and prove such behavior, severe supervisory measures (penalties, responsibility for persons) should limit such cases.

Requirements apply for crypto-asset that are admitted to trading (or a request for admission has been made). This means that it applies for crypto-asset which are traded on trading platforms (or regulated markets). However, it does not matter if a breach of market abuse requirements with such crypto-asset happened on a trading platform, or an outside trading platform (Article 86(2) of MiCA). In other words if a crypto-asset is included in a trading platform, market abuse

manipulation is prohibited for any activity with all crypto-asset services (e.g. exchange, portfolio management).

What is also important to note, is that the market abuse title of MiCA applies for all persons in general. That is, if a person engages into market manipulation, then such persons can be subject to supervisory actions. No matter if it is a private person who otherwise has nothing to do with MiCA.

In order to implement market abuse requirements, a CASP is subject to two groups of requirements:

- Every CASP shall implement measures on inside information and disclosure of inside information (prohibition to trade with inside information and disclosure of inside information), and
- Certain CASPs shall implement arrangements in order that market abuse would be prevented when services are provided.

The following sections will provide details on how CASPs should implement those requirements.

8.1. Inside information

All persons are prohibited to engage into market abuse. This means that if a person is a member of a management body, a shareholder, or an employee of a CASP or offeror, person which seeks admission, then such persons cannot dispose, cancel, amend an order of a crypto-asset to which a person has inside information, including the submission, modifying or withdrawing a bid. Such persons can not recommend or in any other way induce other persons to do that as well. It is also important to note that legal person requirements apply to such employees (persons) who made the decision to hold positions of a crypto-asset on behalf of that legal person. Such persons also cannot disclose information to other third persons.

Inside information is material non-public information. For the information to be considered as inside information, it shall have the following elements:

- Be of a precise nature, (which means that it should be factual information, such as earnings of the company, the launch of new products. Rumors should not be considered as inside information).
- Be non-public information about clients' orders (information should not be disseminated to the public, and known by few persons only, e.g. members of the management body). This includes information regarding the pending orders and applies to persons who are in charge of handling orders at a CASP.
- May influence significantly the price of a crypto-asset (after revealing the information to the public the price of crypto-asset would increase or decrease).

Example of inside information, is changes in management and supervisory boards, decisions to increase or decrease the share capital, legal disputes, changes in expected earnings or losses.

Usually issuers of crypto-asset possess such information. However, under MiCA offerors of crypto-asset, or persons seeking admission to trading, are also subject to inside information requirements, but only to that information which concerns (are related to) them. Such information shall contain inside information about them. In other words a trading platform may also be

subject to disclosure of inside information about their trading platform, if they seek admission of a certain crypto-asset instead of an issuer.

In the event of an inside information situation, the relevant inside information shall be disclosed to the public as soon as possible, on the company website, in the form of a downloadable written statement which is accessible freely to users, and kept for 5 years. Disclosure shall be made as such, and should not be combined with marketing material. Other necessary requirements for making the disclosure are that it shall indicate time and date, be in a language of the white paper and in English, enable the possibility to provide an alert (i. e. newsletter subscription, pop up notification or something similar), be accessible throughout all the EU, and distributed widely and free of charge.

In addition to the website disclosure, this information shall also be communicated by other means, such as by social media, and traditional media. Access to users should not be restricted, and the appropriate website link to the location where the information has been disclosed, shall be provided. There are a few more technical requirements regarding the means of disclosure that are referred to in Article 3 of RTS, on disclosure of inside information.

There may be reasons that the disclosure needs be delayed, where a disclosure would be detrimental to persons for whom this obligation applies. In such cases, it is possible to delay the disclosure of such inside information. Any such delay should not mislead the public, whilst balancing the need for information to remain confidential. In such cases, the issuer, offeror or person who seeks admission to trading, shall inform the competent authority about when the relevant information is to be disclosed to the public, and provide explanation how above mentioned requirements are met (that are set out in Article 88(3) of MiCA). By default, some MS may not hold the requirement to provide information to them, but instead may request this information only explicitly, by contacting that person. National laws and requirements regarding this should be checked (i.e. if MS applied a discretion under Article 88(3) of MiCA).

8.2. Arrangements to prevent market abuse

The market abuse requirements apply for certain CASPs only. CASPs that arrange and execute transactions shall have procedures and systems to detect and prevent market abuse. Persons that arrange and execute transactions are not defined under MiCA, but this is important issue. In conventional case, this means those persons that provide reception and transition, and execution of orders. There may be Q&A under MiCA and those persons will be defined.

Persons that arrange and execute transactions shall provide notifications for competent authorities, STOR notifications, and employ relevant software systems, and must also have in place adequate procedures, along with the sufficient amount of human resources. As an alternative, a CASP can outsource this activity to another person or group entity. Furthermore, particular attention should be given to the training of employees regarding market abuse. Training should be carried out on a regular basis.

Where a market abuse event has been committed, is being committed, or is likely to be committed, by the CASP that professionally arranges and executes a transaction, the CASP shall provide STOR notification to its NCA. The STOR template is provided in Annex of RTS on detection of market abuse. The STOR provided to the NCA should be based on facts and analysis. It means that the STOR should be reasonable. A CASP cannot notify STOR without

being sure that a market abuse case has happened, or is likely to happen. The information (STOR template) should be provided by electronic means specified by each NCA (information can be find on their website), and submitted without delay. Where there is a delay, the CASP should provide information about the past event, along with a suitable explanation to the NCA.

9. Operational requirements

9.1. Best obligation duty

Article 66 of MiCA

A CASP shall act honestly, fairly and professionally, in accordance with the best interests of their clients and prospective clients. There are a subset of requirements that all CASPs should fulfill for this purpose, below is a brief description of them.

9.2. Information for the clients and marketing communication

Article 66(2) of MiCA

Marketing communication shall be fair, clear and not misleading and identified as such. Clients should be able to easily discern what communications are simply advertisements, rather than mandatory information. For example, client information should be easily recognizable where it is marketing communication being provided, and where it is white paper. Even if MiCA does not provide further requirements for marketing communication, they may be set by national legal acts defining either general marketing rules for all sectors, or dedicated for crypto-asset or financial sectors. Therefore a CASP should check the requirements, in the Member States where they intend to provide services.

Regarding information to the clients, a CASP shall warn clients of the risks associated with transactions in crypto-asset.

9.3. Disclosure of white paper

Article 66(3) of MiCA

A CASP will need to provide a hyperlink to a white paper if it provides the operation of a trading platform, exchange, portfolio management, or advice services. There must always be a white paper, so this obligation shall be fulfilled all the times. If there is no white paper such crypto-asset cannot be offered in the EU. Otherwise if a CASP provides a hyperlink with a crypto-asset that is not officially offered in a means that is permitted in the EU, then such CASP is an offeror (requirements of Title II- Title IV of MiCA depending of a type of crypto-asset apply).

9.4. Information of pricing

Article 66(4) of MiCA

A CASP shall publish information about pricing, costs and fees on their website.

9.5. Sustainability

Article 66(6) of MiCA, RTS on sustainability disclosure

In order to allow holders of crypto-asset to compare the environmental impact of crypto-asset, a CASP will need to publish relevant information on their website concerning the adverse impact of climate and environmental factors related to consensus mechanism (PoW, PoS etc). Issuers have on their side an obligation to include that information in the white paper. Requirements and templates for disclosure are specified in the Annex of RTS on sustainability disclosure. Disclosure shall be made free of charge, in a downloadable file, in a way that is easy to read, using characters of readable size, and using a style of writing that facilitates its understanding. Information can be disclosed in English language only. This information shall be updated annually, or at the point where there is a material change (changes should then be made identifiable).

RTS is quite clear on the ability to reuse already available information. This means that a CASP (and issuers) can use information with regards to a disclosure by another entity, so long as that information is reliable. Under normal cases an issuer (or in cases of another person being the producer of a white paper) should disclose all information in the white paper. Therefore a CASP could take that information and publish on its own website, in a form required by RTS on sustainability disclosure, i.e. in a way which allows for an easy comparison of environmental impacts across all the crypto-asset. This means that the chosen presentation format should be in a mode which allows comparison of all crypto-asset.

Only Table 2 of Annex of RTS on sustainability indicators is mandatory for all CASPs. Table 3 is mandatory for a CASP that provides the operation of a trading platform, or exchange service, and where yearly energy consumption exceeds 500,000 kilowatt-hours. In other cases Table 3 is optional. Table 4 is optional for all CASPs.

9.6. Compliance and risk management

Article 68 (4) of MiCA

A CASP shall comply with all requirements at all times. There is no requirement to have a compliance function (i.e. Compliance Officer) for a CASP. However, for a large company, this requirement is likely to come indirectly from Article 68(4) of MiCA. In such case the Compliance Officer could be either a full-time or part-time employee, or otherwise this function could be outsourced. In case of outsourcing, the requirements for outsourcing will therefore also apply. Where this function is established, the Company could have a compliance policy or procedure, which sets out the relevant responsibilities and other arrangements.

Usually the Compliance Officer shall regularly monitor compliance of the implementation of legal requirements, and submit an annual report for the management body concerning compliance and infringements, and any deficiencies identified. To meet the appropriate reporting requirements, a Compliance Officer should make sufficient periodic reports (i.e. monthly and quarterly reports, followed by an annual report, generated from those periodic reports).

The Compliance Officer shall be suitable for the position, which means the person must have the appropriate experience, knowledge, and skills to carry out his or her functions, and must have a

sufficiently good reputation, as well as the ability to maintain independence of this function. The Compliance Officer shall be accountable to the management body, and can only be revoked with its approval. In general this function even in bigger companies, can be merged with other functions.

In addition a CASP shall take strong risks management procedure. CASP shall set risk appetite and ensure that it is aligned with strategic goals. Risk management framework shall include a register of risks and qualitative and quantitative risk assessment.

9.7. Business continuity management

Article 68 (7) of MiCA

In order to ensure the continuity of the main services and activities of the CASP, they shall put in place appropriate procedures for the continuity management process. This process shall focus on IT and ICT continuity, as those areas in most cases, are most important for the continuity of the business.

A CASP shall:

- Draft a policy on business continuity. The Policy shall include a suitable plan (concrete actions) which covers as a minimum, the ICT response and recovery plan under Regulation (EU) 2022/2554.
- The Plan shall be tested regularly. The Policy shall be reviewed by the management body annually.
- Ensure where IT providers of critical and important functions (such as cloud service provider) deliver adequate services (basically by putting certain provisions in the agreements).
- Establish a process for how updates are communicated to employees.

9.8. Record keeping

Article 68(9) of MiCA, RTS on record keeping

A CASP shall keep records of all crypto-asset services and activities, orders, and transactions undertaken by them. Records shall be kept for 5 years, unless MS specified in national laws that records shall be kept for a 7 year period, or make a request during those 5 years.

All lists or records that a CASP hold, shall be kept in accordance with the guidelines specified in the Annex of RTS on records keeping. The Policy developed by a CASP on record keeping should specify the retention period, owners of data, and data destruction measures.

Annex RTS on records keeping specify that such records shall be kept:

- Records on policies and procedures under MiCA, and any audit trails of the assessment, and periodical reviews by the management body (i.e. minutes, agendas, proposals to review).
- Agreements with clients regarding the provision of services.

- Records of clients' crypto-asset that are safeguarded and administered (balances, agreements with credit institution where funds are safeguarded).
- Names and functions of the staff responsible for safeguarding.
- Where it is sub·delegate then agreements and details on such entities.
- Reports about orders and transactions. Records of all transactions (buy/sell crypto-asset). In cases of portfolio management services, then records about the person who takes decisions (i.e. buy/sell crypto-asset) or computer algorithm.

Where a CASP keeps records of transactions of natural persons, the records of those clients shall be identified by ID used in his/her country of nationality. There is a specified format for each country. Where a client is resident of another country other than his/her nationality, then the CASP shall use the country of residence. Legal entities shall be identified by legal entity code. Crypto-asset shall be identified by using a digital token identifier.

9.9. Wind down plan

Article 74 of MiCA

A CASP that provides custody, exchange, trading platform, execution and placing services shall have a plan to support an orderly wind down. The purpose of wind down planning should be to specify the resources (financial and non-financial) needed for wind down, which does not cause any economic damage for the clients. The decision to wind down can be made by the company itself or it can be based on external factors (such as regulatory intervention). The CASP shall have orderly wind-down plan that shall be established taking into account national requirements. The Plan should specify under which circumstances the company will cease its activities, set a process with a suitable timeline for the wind-down, specify required financial recourses, including liquidity. The plan shall include continuity or recovery of any critical activities performed by a CASP, and demonstrate that the CASP will be able to cease its activities. The plan shall be drafted in accordance to national requirements, if any.

9.10. Significant CASPs

Article 85 or MiCA

There is a separate category of CASPs that are considered to be a significant CASP. A CASP is considered as significant if it has on average at least 15 million active users in a calendar year, registered as a daily number of active users (i.e. 15 million users should log in or interact with a CASP daily). Such CASPs are subject to additional reporting obligations to the NCA. Then ESMA is informed about certain supervision practices by home NCA of such a CASP.

9.11. Reporting and accounting and CRS

MiCA does not specify requirements for the organization of the chosen accounting method of the CASP. A CASP can use national accounting standards or IFRS. However, national laws may set requirements for certain types of companies to conduct the accounting using specific accounting standards. Each CASP should check the national requirements of the Member State where they are established.

A CASP shall have in place an accounting policy or procedure, where it describes the main accounting principles and methods used. One of the main elements of this is to describe extraordinary principles or methods, or options allowed by accounting standards. The Accounting Policy or Procedure shall state the period when the Company's accounting year starts and ends.

The fixed overheads requirement is calculated using applicable accounting standards. Where the requirement is high and the Company has a choice (i.e. national accounting standards have not set any requirement to do accounting using IFRS or national) a CASP can consider this. However, since there may be significant deviation this could lead to significant changes to the required amount of own funds. In such cases it is recommended to use both accounting standards, and to see if the difference is significant.

Currently there are no prudential or periodic activities reporting under MiCA. Some member states could though introduce national reporting requirements.

Common reporting Standard (CRS) is information that a CASP needs to report for tax authorities which exchange this information among each other. It is not part of MiCA. Requirements are set by Directive (EU) 2023/2226 and Regulation (EU) 2022/1467.

10. Service specific requirements

10.1. Custody and administration

Article 75 of MiCA

When a CASP safe-keeps and administrates clients' crypto-asset or the means to access them (i. e. private keys), or funds, it shall ensure that in case of insolvency ownership rights will be ensured to the clients, and the CASP shall not use funds for their own account. Funds must be deposited in a central bank (which is not possible at the moment since central banks do not open accounts for CASPs) or credit institution, by the end of the next day when funds were received. Accounts where clients' funds are held shall be separate from the CASPs own account.

The most important requirement is that any crypto-asset and/or funds held on behalf of the clients should be segregated from crypto-asset that belong to the CASP itself. This requirement is introduced so that any claim from third parties would not be for client assets in case of CASP insolvency.

Where a CASP provides custody and administration, the CASP shall have a written agreement with its clients, and the agreement shall include all elements of Article 75(1) of MiCA, as well as details of a Custody policy. A summary of the policy shall be provided to the clients on their request.

A CASP shall keep records that enable a client's asset to be segregated from other clients' assets, at all time, and be able to do reconciliations. Once a quarter the CASP shall provide a report on the client's balance of account, as well as on transactions during the reporting period. Upon a client request, information should be provided on an ad-hoc basis.

A CASP shall have records of all positions of each client's crypto-asset positions for which it provides safeguarding and administration services.

Where a CASP itself is responsible for the loss of a client's assets (for example due to ICT event) then the CASP is responsible for compensation of such assets to the clients, at market value.

A CASP can sub-delegate custody to other authorized entities. Where the CASP sub-delegates, it shall have measures to assess due diligence and obligations of the entity for which it has delegated.

A CASP cannot use crypto-asset or funds belonging to the clients on their own account. For example, they cannot lend clients crypto-asset on the benefit for their own account. This is related to staking in one of the activities which involves a client's crypto-asset under custody. Staking is not regulated under MiCA. However there is a rule that a CASP cannot use a client's asset in its our account. Staking most probably would not fall under the use of own account for a client's assets if the client gets a reward and the assets are not incumbered. Besides, Article 75(4) of MiCA requires that clients' rights are created (which might cover staking) or modified so that the client shall be entitled to new crypto-asset or rights. But the CASP can have a provision in the agreement with clients that allows for not transferring rights or crypto-asset to the client.

10.2. Operation of trading platform

Article 76 of MiCA

Trading platforms are allowed to accept retail users, therefore retail clients can interact with them without intermediaries. The most important requirement for them is to ensure that only MiCA compliant crypto-asset are admitted to trading, and to ensure pre and post trade transparency (information about orders, quotes).

A CASP shall put in place procedures regarding the admission of members on their platform. Members admission rules shall be based on admission procedures.

They cannot admit a crypto-asset if there is no white paper.

CASPs operating a trading platform for crypto-asset, shall not deal through their own account on the trading platform for the crypto-asset they operate, including where they provide the exchange of crypto-asset for funds or other crypto-asset. This is an important requirement to avoid a conflict of interest. In addition, from a client's perspective, clients can be sure that they are offered a fair price. But despite that CASPs can engage in matched principle trading (align clients' orders where the trading platform is buyer and seller from two different clients with no market risk or profit or loss). In such cases clients shall give a permission (requirements not mentioned how so either explicit or implicit). Explanation for NCA should be provided for how this model will work.

Pre and post trade transparency requirements apply. Post trade transparency means that the CASP shall make public any bid and asking prices, and the depth of trading interests at those prices which are advertised for crypto-asset, through their trading platforms on a continuous basis during trading hours. Post trade transparency means that the CASP shall make public the price, volume and time of the transactions executed in real time. There is no deferral time in post

trade transparency. This information shall be made available free of charge 15 minutes after publication in a machine-readable format and it shall remain published for at least two years. During those 15 minutes information can be made available on a commercial basis.

To ensure settlement finality on orders, the maximum settlement time after the execution time, is set to 24 hours or by 1 hour after the close of the day, if transactions are outside of a blockchain. This should be looked at whilst taking into account the technical capabilities of a particular blockchain.

10.3. Exchange of crypto-asset to funds or other crypto-asset

Article 77 of MiCA

Where a CASP provides exchange services, the CASP shall prepare a non-discriminatory commercial policy. This policy in general shall outline the type of clients for whom the CASP provides exchange services, and any conditions for its clients. It could include provisions such as; if clients are not onboarded the CASP does not provide services to them, or conditions for when and how clients can access the services provided by the CASP and where services may not be available. Even if MiCA does not set requirements to publish this Policy, it would be rational to do so, from the clients' perspective.

For crypto-asset where they provide exchange services, a CASP shall either publish on its website a firm price (i.e. price itself) or a method for determining the price (i.e. price methodology). Besides if there is a limit on the amount that a client can exchange, this limit shall be published as well (i.e. if client in one transaction can exchange of max 1 000 euro equivalent amount or overall limit). Price or methodology should be published on the company website publicly. This will ensure price transparency for the whole market.

Transactions shall be executed at the prices displayed at the time when the order is final. The CASP shall inform the client when the order is final (i.e. will be executed).

There are so called post trade requirements. A CASP shall publish volume and prices of transactions executed by them. Further requirements are not defined and this may be subject to wide interpretation. Trading platforms have the requirement to publish volume, price and time and in real time. Meanwhile since it is the case for CASPs that provide exchange services, to publish information about the time is not required, it could be considered that daily publication could be sufficient. This information shall remain for sufficient time, as mentioned by ESMA Q&A, at least by midnight of the following business day.

10.4. Execution of order

Article 78 of MiCA

The key obligation for a CASP is to ensure that clients' orders are executed on the best execution basis. Best execution is where a client's order is executed taking in to account price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-asset, or any other considerations. In general best execution in standard cases means best price (overall, with fees) execution. But when clients can give specific instructions in the order (for example specific execution place) then best execution criteria does not apply because the clients instructed otherwise.

The order shall be executed promptly and information on pending orders shall not be misused.

A CASP shall draft the best execution policy. There is no requirement to disclose this policy publicly, only a summary/sufficient details shall be disclosed. The Policy shall specify venues of order execution and the overall procedure.

A CASP shall regularly assess the best execution. This means that there is a requirement to be able to demonstrate to clients and competent authorities, the best execution. For this the CASP needs to implement a monitoring arrangement.

In general, orders shall be executed on a trading platform. However if a CASP executes orders outside of a trading platform it shall get consensus from the client, either is general form or for an individual order. This applies if a CASP executes orders using a CASP that provides an exchange service. CASPs are prohibited to receive any financial or non-financial benefit for routing the order for the execution to or from other CASPs. It is so called payment for order flow prohibition.

10.5. Placing of crypto-asset

Article 79 of MiCA

Placing is the service where a CASP markets (promotes) in the EU, a crypto-asset that is issued by other persons. It is the commitment to market the crypto-asset on behalf of the issuer, offeror or other person. Where a CASP provides that service it shall have an agreement with the issuer, offeror or other persons for whom they offer placing services. The agreement shall indicate the type of placement (i.e. whether the CASP guarantees that a minimum amount will be purchased), fees of transactions, the likely timing, process and price for the proposed operation, and information about the targeted purchasers.

Where placing services are provided in addition to other crypto services, there is potential for a conflict of interest situation. Therefore additional requirements for conflict of interests apply, with regards to placing services where the CASP places crypto-asset for its client (i.e. provides portfolio management and includes this asset in clients' portfolios), or where there is proposed price estimation, or where monetary or non-monetary benefit is granted by the offeror.

10.6. Advice

Article 81 of MiCA

Advice on crypto-asset can be one of two types – one time (where a client asks for this service on a one-off basis) or ongoing (where the CASP review results from advice, and clients receive this service on a continuous basis.) Advice can be both independent and dependent. Independent advice is where a CASP offers advice to the client on a product, based on broad market analysis and is unbiased. Clients are better off when they receive independent advice because they may be offered a broader range of products. Therefore there are several additional requirements where a firm provides advice on a dependent basis.

In general, advice is understood as the provision of a recommendation exclusively for a client, and involves the assessment of client's circumstances, and leads to an action (to buy, sell, hold) regarding a concrete crypto-asset. For example, in situations where someone on social media

gives information to a group of clients about concrete crypto-asset and indicated the signal of buy, then such actions could be considered as crypto-asset advice.

Requirements for CASPs that provide crypto-asset advice:

- To assess the suitability of crypto-asset advice (i.e. to carry out a suitability test) for each client. The test shall assess three elements about the client: client's knowledge and experience, objectives, risk tolerance, financial situation and ability to bear losses (Article 81(1) of MiCA). If the results of the test indicate that the crypto-asset (or a type of crypto-asset) is not suitable for a client, then the CASP should not recommend such crypto-asset for the client. The test shall be completed and documented before the provision of crypto-asset advice. The CASP shall have policies and procedures on suitability assessment test (i.e. a Suitability Test Assessment Policy).
- Provide information for clients to indicate whether advice is independent or dependent, and whether it is based on a broad or on a more restricted analysis of different crypto-asset, in particular when advice is issued by closely related entities to the CASP.
- For dependent advice a CASP can receive inducements (monetary payments or other benefits, such as invitation to a conference, payment of a flight ticket) but shall clearly disclose that to the potential clients (i.e. before the provision of this service). Besides, payment or benefit shall be designed to enhance the quality of the relevant service to the client (example could be a discount that is useful for clients, or research material which is also useful).
- Meanwhile where a CASP provides independent advice, it assesses a broad range of products in the market. In does not mean that a CASP needs to assess all available crypto-asset in the market in order to recommend them to clients. It would not be possible to do that. However this means that the assessment should be independent (does not rely on closely linked entity's products). In such cases the CASP cannot accept fees, commissions or other benefits by third parties (i.e. other entities whose products a CASP recommends for its clients). Minor non-financial benefit can be accepted (i.e. invitation to the conference), but shall be disclosed to the clients.
- Provide detailed information on costs and fees in advance, for potential clients.
- Persons who provide advice to clients must possess the necessary knowledge and competence to fulfill their obligations (i.e. be qualified to provide advice).
- Provide warnings to the clients such as that the value of crypto-asset may fluctuate, maybe be illiquid, are not subject to deposit insurance or investor protection schemes.
- Shall report to the client how the advice given meets the suitability of the clients.

Suitability test assessment is specified under MiCA and ESMA Guidelines on suitability assessment. The most important thing is to ensure that clients are informed about the purpose of the test and the CASP should ensure that clients provide (or are informed) about the need to provide the CASP with the necessary information. Information collected from the clients should be reliable. It is recommended to regularly re-assess this at least every two years.

10.7. Portfolio management

Article 81 of MiCA

Portfolio management is the service where a CASP manages clients' portfolios of crypto-asset according to in advance defined mandates (rules).

Where a CASP provides a portfolio management service it shall:

- To assess the suitability of crypto-asset portfolio management (i.e. to carry out suitability test) for each client (as it is explained above regarding the provision of crypto-asset advice).
- It is prohibited to take any monetary or non-monetary inducements (payments or other benefits, including investment research) from third parties in all cases.
- Provide quarterly statements for the clients (can be accessed by clients on the website/app). Requirements for reports are specified in the Guidelines on suitability assessment.

10.8. Reception and transmission of orders for crypto-asset on behalf of clients

Article 80 if MiCA

This service requires that crypto-asset would be received and then transmitted to another entity for the execution (or further RTO). This is considered as MiCA service if both elements are in place (i.e. orders are received and then transmitted). Where an order is received a CASP shall transmit it to a trading venue or other CASP immediately.

The CASP cannot receive any financial or non-financial benefit for routing the order from trading venues of other entities to which they route the client order. It is so called payment for order flow prohibition, just under normal cases it should be prohibited for the execution of order, not RTO.

Information about pending orders shall not be misused by a CASP or its employees and CASP shall prevent that.

10.9. Transfer service

Article 82 of MiCA

Transfer service may be provided in combination with other services. Since this service is similar to payment service under Directive 2009/110/EC, and EMTs are e-money tokens for which this directive applies, there may be overlap of those services and CASP should access if they need the authorization under MiCA to provide this service.

The main requirement here, for a CASP, is to have an agreement in place with its clients. There are additional requirements under the Guidelines on Transfer Service that cover basically the provision of the information for the clients and what information shall be included in the agreement. A CASP should pay attention to the Regulation (EU) 2023/1113 and whether the information is accompanied by requirements in Article 14 of the requirements.

The requirements regarding the provision of transfer service are as follows:

- CASPs shall have an agreement with their clients regarding the provision of the transfer service. The Agreement shall be sufficiently detailed, and shall contain at least the following information: the identity of the parties to the agreement, a description of the modalities of the transfer service provided, a description of the security systems used by the crypto-asset service provider, fees applied by the crypto-asset service provider, and the applicable law. Similar agreements are publicly available for e-money institutions, so

a CASP can check for those examples. The agreement should be published on the CASPs website or communicated for the clients in advance, because there is a requirement to provide it for the clients in good time, before the provision of the transfer service, and a copy shall be provided to the clients. Agreement should specify the liability of the CASP in case of unauthorized or incorrectly initiated or executed transfers of crypto-asset.

- The information that the CASP shall provide for the clients is listed in point 12 of the Guidelines of Transfer Service. The information includes information on the CASP, nature of the service, technical information on the transfer, all charges, fees or commissions and any other relevant information. Essentially, all such requirements could be included in the agreement with the client. This information shall be accessible at all times for clients, or on a client's request.
- Where there are amendments to the information the client shall be made aware of those changes in advance.
- After the reception of an instruction to transfer crypto-asset, but before the execution of the transfer of crypto-asset, the CASP shall provide the client a warning, if the transfer is irreversible or sufficiently irreversible in case of probabilistic settlement, along with information about the charges. The information about the charges can be referred as a link to the website.
- Before the provision of the service the CASP shall ensure that clients are verified and onboarded, and have completed KYC and AML/TC procedures.
- After the execution of the transfer transaction a CASP shall provide the client all information listed in point 19 of the Guidelines. Such information can be provided as an email confirmation, or in any other form.
- A CASP should also include in the agreements, the relevant technical information regarding cut off time, if applicable. Cut off time means the time when the execution of the transaction would be made in the following business day. In addition, relevant information regarding the maximum execution times depending on the crypto-asset transferred, and the number of block confirmations needed for the transfer of crypto-asset to be irreversible on the DLT, or sufficiently irreversible in case of probabilistic settlement, for each DLT network.
- A CASP should have systems in place that reject or suspend the transfers, measures of how to execute, reject, return or suspend a transfer of crypto-asset for money laundering and terrorist financing purposes. In general such procedures should cover cases where a transfer is suspended due to the client is being subjected to AML/TR risks, and for what actions will be taken then. In such cases the CASP shall provide the client with the reason for the rejection, how to remedy the rejection, return or suspension, the amount of any charges or fees incurred by the client, and whether reimbursement is possible. In general it could be sufficient for the information to be provided in the agreement as well.

For the purpose of authorization, A CASP should provide its NCA with the following information:

- A copy of the client agreement.
- Identify types on crypto-asset. This information could cover a list of crypto-asset, or could be of a more narrow nature and refer to the MiCA classification of crypto-asset (like ART, EMT, or other crypto-asset).
- ICT risk management. For this a CASP could refer to its ICT procedures, or indicate any other particular technical ICT measure regarding the transfer service. The key requirement is to ensure that any transfers will reach their final beneficiaries.
- Indicate if a CASP has in place an insurance policy, which is optional, not mandatory. If the CASP does have a policy in place, it should also indicate the relevant details of the

policy (i.e. insurance's coverage of detriment to client's crypto-asset that may result from cyber security risks).

11. Provision of crypto-asset services at the exclusive initiative of the client (reverse solicitation)

Article 61 of MiCA

All CASPs that intend to provide crypto-asset services in the EU shall seek authorization under MiCA. However for some it won't help for CASP to avoid MiCA requirements. Reverse solicitation regime means that a third country firm (that is not established in an EU country) can provide crypto-asset services for a limited number of clients without authorization. The purpose of this regime is to leave the possibility for all EU citizens to access the services and products from third country firms, if such persons seek those services and products themselves. Thus a third country firm, in such cases, does not solicit EU clients. For example, professional clients (an investment firm, a bank) can request services and approach a third country firm themselves. However, in such cases the third country firm cannot offer other products or services to those clients. If a third country firm were though to be in a situation where it would have hundreds of thousands of EU retail clients, who all invest small amounts, then it would be quite hard for that firm to explain how so many clients had found out about that company, and approached it independently.

Where clients approach third country firm themselves, the third country firm can provide only those services and offer only those products for which the persons have approached the firm. It means that firm cannot offer other services or products to that client. Paragraph 32 of the Guidelines on reverse solicitation has specified what is considered as other types of crypto-asset.

It is not easy to prohibit such activity, especially when taking into account the inherent global nature of the current crypto-asset market. So Guidelines on reverse solicitation state that essentially all marketing and communication addressed to the EU market by a third country firm shall be considered under the very broad definitions of those Guidelines. Simply put, if a firm's logo is visible in the EU due to sponsorship deals, then this fact alone may restrict the firm's ability to use the reverse solicitation regime. If a firm raises awareness in the EU (e.g. it's logo is demonstrated during an international broadcasting event) but it does not intend to provide crypto-asset services in the EU, then that firm needs to take relevant action, for example, to block their website in the EU area so that clients cannot see information and access its services.

This applies to group entities or where another entity redirects clients as well. Usually from a practical perspective it is not possible to overcome this regime, for example by directing clients to group entities that are established outside the EU. Besides when a third country firm would like to use this regime, it is required to maintain appropriate records that can show that the clients approached the firm itself, in order to be able to prove that fact to supervision authorities.

Supervision authorities take actions when a third country firm provides services to EU clients without proper authorization. As stated in the Guidelines, NCAs should have appropriate

measures and react to warnings in their home MS. There are currently no harmonized practices with regards to what actions each NCA takes, however, Article 94 of MiCA provides them with supervisory powers.

MiCA does not have specific categories of clients. Instead there is only one category of clients. So this means that there is not a separate category for professional clients, or a category for retail clients, as is the case under MiFID. Under MIFID it is considered that professional clients are more sophisticated, and therefore it is seen that there is no need to protect them to the same extent as retail clients, so firms providing services to professional clients under MIFID, are exempted from some of the requirements. In contrast though, under MiCA where professional clients will seek services from a third country firm, firms should take this into account, and so careful records about all clients should be maintained, including professional ones (i.e. a CASP itself).

12. Passporting

Article 59(7) of MiCA

Once authorized in one MS, a CASP can provide crypto-asset services in other member states by:

- using freedom to provide services on a cross border basis (passporting) regime,
- establishing a branch in another member state.

The Passporting regime is the simplest way that allows a CASP to provide crypto-asset services in all of the EU. Basically a CASP should provide a simple notification document for the national competent authority where a CASP is established, either when applying for an authorization or at later stage when the CASP already has a license. It is more efficient to ask for it together with an authorization. The notification document shall contain a list of member states intended to provided services in, indicate which crypto-asset services will be provided, starting date, a list of all other activities provided by the CASP that is not covered by MiCA. A notification template should be published by each national competent authority.

Upon receiving a passporting request from a CASP, the receiving NCA shall transfer that notification to the national competent authorities in which the CASP intends to provide cross border services, within 10 working days. A CASP can start to provide services on a cross border basis, i.e. in other MS, when it receives a communication from its competent authority, or after 15 working days from when it submitted the notification document if the NCA has not yet replied. No other requirements apply, there is no requirement to have a physical presence in that member state.

A CASP can also establish a branch and provide services through a branch in another MS. Then that MS should not add additional requirements to such CASP. Since there are no specific requirements under MiCA regarding the establishment of a branch, it means that national laws of EU MSs regulate that procedure. Typically it can be expected to be a longer procedure than the passporting notification.

13. Other information

- There will be a black list of CASPs that provide services in the EU without authorization, or in violation of MiCA. ESMA will publish and maintain this list.
- There may be product intervention by NCAs. Product intervention means that an NCA may prohibit to market certain crypto-asset in the EU, or to provide certain services for CASPs.
- NCAs handle complaints between clients and other interested parties, including consumer associations and CASPs.
- ESMA will establish a list of all white papers.
- There are two types of supervision models – off site (i. e. reviewing reports and activity of a CASP based on information, signals) and on site supervision (where NCA comes to the premises of the CASP. Each NCA has its own system.
- Supervisory fees are set by each supervision authority (NCA). In each MS they will differ.
- By 31 December 2025 and 2027 there will be quantitative report on crypto-asset.
- By 30 December 2024 there will be report on DeFI, lending and borrowing, transfer of e-money tokens service, development of NFT.
- Other regulations that are relevant is Regulation (EU) 2023/1113 on transfer of funds, Common Reporting Standards mentioned briefly under the accounting section.