**Notification form for the provision of Crypto-Asset Services under Regulation (EU) 2023/1114**

**Reference number:** …………….

**Date:** ……………………………………

**FROM:**

Name of the notifying entity:

Address:

(Contact details of the designated point of contact)

Name:

Status/Position:

Telephone:

E-mail:

**TO:**

The Dutch Authority for the Financial Markets (**AFM**), Vijzelgracht 50, 1017 HS Amsterdam

By mail: crypto@afm.nl, for the attention of the MiCAR supervisory team

Dear AFM,

In accordance with Commission Implementing Regulation (EU) 2024/XXX, laying down implementing technical standards for the application of Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to standard forms, templates and procedures for the notification of certain entities of their intention to provide crypto-asset services, kindly find attached our notification of our intention to provide crypto-asset services.[[1]](#footnote-2)

**Guidance from AFM**

It is important that the notifying entity submits a complete and correct documentation package that is of good quality. This will reduce the need for iterations and result in a more efficient notification procedure for both the AFM and the applicant. The **notification form** should contain a clear argumentation of how the applicant complies with the rules in Regulation (EU) 2023/1114 (**MiCAR**) and include supporting documents to substantiate this.

The notification form contains *in italics* guidance on the information or supporting documentation that we expect from the notifying entity. Please use the checklist (downloadable from our website) to provide information of the contents of the supporting documents and please make sure to include an overview of provided documents, including references to the related question of the application form. Please note that the answers, as well as the supporting documentation may be provided in either Dutch or English.

Additionally, please include a **cover note** that includes a letter from management and highlights any points that you want to draw attention to.

**Further remarks:**

Please pay close attention to the following:

1. To submit a notification, the notifying entity must use this notification form and provide the required enclosures with this form. Please ensure the latest version of this form is downloaded from the AFM website.
2. The completed notification form, together with the cover note, checklist and supporting documentation must be sent to crypto@afm.nl by email [with use of Cryptshare](https://www.afm.nl/en/contact/veilig-bestanden-uitwisselen). This ensures a secure file exchange. Please make sure to send the Cryptshare password in a separate mail.
3. The AFM will only process a notification if the notification form is completed fully and legally signed on behalf of the notifying entity.
4. The AFM reserves the right to request additional information and/or documentation.
5. A fee is charged by the AFM to the notifying entity for making the notification. An invoice will follow shortly after the assessment of the notification is complete, regardless of the outcome. The AFM will also charge a fee if the application is withdrawn by the applicant.
6. If circumstances as stated in the notification form change during the notification process, the AFM must be informed of this in writing without delay. Any such changes must be submitted via mail to your contact person at the AFM with crypto@afm.nl in CC.
7. Supporting documentation should have a clear naming convention that includes an exact reference to the related topic and/or question, following the example below. The AFM is not unable to process supporting documentation that is not sufficiently named and referenced. Furthermore, please place supporting documentation in subfolders corresponding with the question number in the application form.

Example of a document name:

“question 6\_custody\_and\_administration\_policy”

1. Various questions include a request for a “description”. Please provide a concise but accurate description of the requested information and, optionally, specific references to supporting documentation (e.g., chapter and page numbers). We note that the information in the notification form is leading for our assessment, whereas the supporting documentation should provide the underlying evidence for the provided answer of MiCAR-compliance on the relevant topics. Please ensure that your answers in this form are self-explanatory. We note that solely referring to annexes is not considered a self-explanatory answer. Furthermore, if you deem a question not applicable to your situation, please provide the reason why.
2. Since not all the requirements have not been finalized, the applicable rules may be subject to change. You should therefore always consult the most recent publications of the applicable regulations. You may also engage an advisor with experience of MiCAR or other licence applications or notifications. However, the obligation to comply with the requirements of CASPs remains with the applicant.
3. Please consider the latest available supervisory guidance when filling in the notification form, such as published AFM Frequently Asked Questions (FAQs) and ESMA Questions and Answers (Q&A’s) which can be found on the websites of the AFM ([see link](https://www.afm.nl/en/sector/cryptopartijen/contact-qa)) and ESMA ([see link](https://www.esma.europa.eu/publications-and-data/questions-answers)).

If any questions remain, please send an email to crypto@afm.nl.

**Signature**

|  |
| --- |
| We [notifying entity] declare that the submitted information is true, accurate, complete, not misleading and to the best of [notifying entity’s] knowledge.Place Date Name of person in charge of day-to-day operations Signature of person in charge of day-to-day operations |

**Notification form for the provision of Crypto Asset Services**

## **Programme of operations**

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

|  |  |  |
| --- | --- | --- |
| **A** | **Where the notifying entity belongs to a group, an explanation of how the activities of the notifying entity will fit within the group strategy and interact with the activities of the other entities of the group, including an overview of the current and planned organisation and structure of the group** | *Please also provide a detailed organigram of the holding structure of the applicant, including the breakdown of its capital and voting rights and the names of the shareholders or members with qualifying holdings.* |
| **B** | **Explanation of how the activities of the entities affiliated with the notifying entity, including where there are regulated entities in the group, is expected to impact the activities of the notifying entity. This explanation shall include a list of and information on the entities affiliated with the notifying entity, including where there are regulated entities, the services provided by these entities (including regulated services, activities and types of clients) and the domain names of each website operated by such entities** | *Please include the business plan relating to the crypto-asset services you (intend to) provide, including the revenue and cost model of each crypto-asset service.* |
|
| **C** | **List of crypto-asset services that the notifying entity intends to provide as well as the types of crypto-assets to which the crypto-asset services will relate** | *Please provide clear argumentation on which crypto-asset services you (intend to) provide (including legal substantiation of the regulatory scope of your activities).* |
| **D** | **Other planned activities, regulated in accordance with Union or national law or unregulated, including any other services, than crypto-asset services, that the notifying entity intends to provide** | *Please include whether you (intend to) provide (i) any staking and/or lending services, or (ii) non-custodial wallets to clients.* |
| **E** | **Whether the notifying entity intends to offer crypto-assets to the public or seek admission to trading of crypto-assets and if so, of what type of crypto-assets** |  |
| **F** | **List of jurisdictions, in and outside the European Union, in which the notifying entity plans to provide crypto-asset services, including information on the domicile of targeted clients and the targeted number by geographical area** | *Please include information regarding services that are offered within as well as outside the European Union (EU). With regard to non-EU jurisdictions, please specify which crypto-asset services are provided and which regulatory framework applies to those services.* |
| **G** | **Types of prospective clients targeted by the notifying entities’ crypto-asset services** | *Please include the current and prospective number of active clients (i.e., at least one transaction in the last 12 months) that you have in each EU-jurisdiction.* |
| **H** | **Description of the means of access to the notifying entity’s crypto-asset services by clients, including all of the following:** |  |
|  | **i. the domain names for each website or other ICT-based application through which the crypto-asset services will be provided by the notifying entity and information on the languages in which the website will be available, the types of crypto-asset services that will be accessed through it and, where applicable, from which Member States the website will be accessible** |  |
|  | **ii. the name of any ICT-based application available to clients to access the crypto-asset services, in which languages it is available and which crypto-asset services can be accessed through it** |  |
| **I** | **Planned marketing and promotional activities and arrangements for the crypto-asset services, including:** |  |
|  | **i. all means of marketing to be used for each of the services, the means of identification that the notifying entity intends to use and information on the relevant category of clients targeted and types of crypto-assets** |  |
|  | **ii. languages that will be used for the marketing and promotional activities** |  |
| **J** | **Detailed description of the human, financial and ICT resources allocated to the intended crypto-asset services as well as their geographical location** |  |
| **K** | **The notifying entity’s outsourcing policy and how it was adapted to crypto-asset services as well as a detailed description of the notifying entity’s planned outsourcing arrangements, including intra-group arrangements, how the notifying entity intends to comply with the requirements set out in Article 73 of Regulation (EU) 2023/1114. The notifying entity shall also include information on the functions or person responsible for outsourcing, the resources (human and ICT) allocated to the control of the outsourced functions, services or activities of the related arrangements and on the risk assessment related to the outsourcing** | *Please also provide an outsourcing register and exit strategies.* |
| **L** | **List of entities that will provide outsourced services for the provision of crypto-asset services, their geographical location and the relevant services outsourced** |  |
| **M** | **Forecast accounting plan including stress scenarios at an individual and, where applicable, at consolidated group and sub-consolidated level in accordance with Directive 2013/34/EU. The financial forecast shall consider any intra-group loans granted or to be granted by and to the notifying entity** |  |
| **N** | **Any exchange of crypto-assets for funds and other crypto-asset activities that the notifying entity intends to undertake, including through any decentralised finance applications with which the notifying entity wishes to interact on its own account** |  |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

## **Business continuity**

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

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

|  |
| --- |
| *Please provide the requested description under question 5-2 in this box.**In your business continuity plan, please also include a scenario that accounts for situations where a (public or private) distributed ledger relevant to the offered services malfunctions and specify how the core activities of the CASP are affected and how these effects are handled.**In the provided documentation package, please also include a:** *Business impact-analysis and risk assessment (Article 11(5) of Regulation (EU) 2022/2554 as used in DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 24, 25 and 26).*
* *Business continuity management policy and Business continuity management procedure (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 24,25,26).*
* *Disaster recovery policy and Disaster recovery procedure (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 25,26).*
* *Back-up and recovery policy and Back-up and recovery procedures (DORA article 12).*
 |

##

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

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

|  |  |  |
| --- | --- | --- |
| **A** | **Notifying entity’s assessment of the inherent and residual risks of money laundering and terrorist financing associated with its provision of crypto-asset services, including the risks relating to the notifying entity’s customer base, to the services provided, to the distribution channels used and to the geographical areas of operation** | *Please also provide an up-to-date Anti-Money Laundering (AML) and Sanctions policy and Systematic Integrity Risk Analysis (SIRA), including information on compliance with Regulation (EU) 2023/1113 (Transfer of Funds Regulation, TFR).* |
| **B** | **Measures that the notifying entity has or will put in place to prevent the identified risks and comply with applicable anti-money laundering and counter-terrorist financing requirements, including the notifying entity’s risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities** | *At least the following topics should be covered in the applicant’s policies:* * *the measures in place to identify and verify the customer and its UBOs;*
* *the measures in place in order to determine whether a client or its UBO is a PEP;*
* *the measures in place to establish whether the natural person representing the client is authorized and to identify this person and verify their identity.*
* *the measures in place to establish the purpose and intended nature of the business relationship;*
* *the measures in place to establish whether simplified customer due diligence is sufficient or enhanced customer due diligence is necessary;*
* *if applicable the delegation of customer due diligence to third parties.*
* *the process of monitoring the relationship and the transactions, if necessary with review of the source of the funds used in the relationship or for the transactions;*
* *the process reporting of suspicious transactions or activities;*
* *the measures in place to train employees and day-to-day policymakers;*
* *the measures in place to record, archive and retain relevant information and documents;*
* *the measures in place to avoid acting in contravention of the sanctions regulations.*
 |
|
| **C** | **Detailed information on how such mechanisms, systems and procedures are adequate and proportionate to the scale, nature, inherent money laundering and terrorist financing risk, range of crypto-asset services provided, the complexity of the business model and how they ensure the notifying entity’s compliance with Directive (EU) 2015/849 and Regulation (EU) 2023/1113** |  |
| **D** | **Identity of the person in charge of ensuring the notifying entity’s compliance with anti-money laundering and counter-terrorist financing obligations, and evidence of the person’s skills and expertise** |  |
| **E** | **Arrangements, human and financial resources devoted to ensure that staff of the notifying entity is appropriately trained in anti-money laundering and counter-terrorist financing matters (annual indications) and on specific crypto-asset related risks** |  |
| **F** | **Copy of the notifying entity’s anti-money laundering and counter-terrorism policies and procedures and systems** |  |
| **G** | **Summary document outlining changes that have been made to the notifying entity’s anti-money laundering and counter-terrorism policies and procedures and systems as a consequence of the planned crypto-asset services**  |  |
| **H** | **Frequency of the assessment of the adequacy and effectiveness of such mechanisms, systems and policies and procedures as well as the person or function responsible for such assessment** |  |

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

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

|  |  |  |
| --- | --- | --- |
| **A** | **Technical documentation of the ICT systems, on DLT infrastructure relied upon, where relevant, and on the security arrangements. The applicant shall include a description of the arrangements and deployed ICT and human resources established to ensure that the applicant complies with Regulation (EU) 2022/2554, including, but not limited to:** | *Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *Information security policy and measures (DORA article 2, 3, DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 29).*
 |
|  | **i. sound, comprehensive and well–documented ICT risk management framework as part of its overall risk management system, including a detailed description of ICT systems, protocols and tools and of how the applicant’s procedures, policies and systems to safeguard the security, integrity, availability, authenticity and confidentiality of data in accordance with Regulation (EU) 2022/2554 and Regulation (EU) 2016/679** | *Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *IT Risk management policy (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 3)*
* *ICT change management policy and ICT change management procedures (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 16, 17).*
* *IT landscape overview.*
* *Technical description of IT infrastructure and ICT systems.*
 |
|  | **ii. an identification of ICT services supporting critical or important functions, developed or maintained by the applicant, as well as those provided by third-party service providers, a description of such contractual arrangements (identity and geographical location of the providers, description of the outsourced activities or ICT services with their main characteristics, copy of contractual agreements) and how they comply with Article 73 of Regulation (EU) 2023/1114 and the Chapter V of Regulation (EU) 2022/2554** | *See also point K under 2. Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *Present policies and procedures related to the third party ICT-risks. These policies and procedures must comply with the:*
	+ *RTS to specify the policy on ICT services supporting critical or important functions (article 28(10)), in compliance with Regulation (EU) 2024/1773)*
	+ *ITS on the register of information (article 28(9), in compliance with Regulation (EU) 2024/2956)*
	+ *RTS on subcontracting ICT services (DORA article 30(5))*
 |
|  | **iii. a description of the applicant’s procedures, policies, arrangements and systems for security and incident management** | *Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *Incident management policy and Incident management procedures (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 22,23)*
* *Access control policy (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 21)*
* *Identity management policy and Identity management procedures (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 20)*
 |
| **B** | **Cybersecurity audit realized by a third-party cybersecurity auditor having sufficient experience in accordance with [DORA TLPT RTS detailing the minimum requirements on capabilities which are described in DORA Level 1 Article 27] covering: the following audits or tests performed by external independent parties:** |  |
|  | **i. organisational cybersecurity, physical security and secure software development lifecycle arrangements** |  |
|  | **ii. vulnerability assessments and scans, network security assessments** | *Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *Vulnerability and patch management procedures (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework 15 article 10).*
 |
|  | **iii. configuration reviews of ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554** | *Please provide a self-explanatory answer in this box and at least also the following supporting documentation:** *ICT asset management policy (DORA RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework article 4,5).*
 |
|  | **iv. penetration tests on the ICT assets supporting critical and important functions as defined in Article 3(22) of Regulation (EU) 2022/2554, in accordance with all the following audit test approaches: - black box: the auditor has no information other than the IP addresses and URLs associated with the audited target. This phase is generally preceded by the discovery of information and the identification of the target by querying domain name system (DNS) services, scanning open ports, discovering the presence of filtering equipment, etc.****- grey box phase: auditors have the knowledge of a standard user of the information system (legitimate authentication, “standard” workstation, etc.). The identifiers can belong to different user profiles in order to test different privilege levels****- white box phase: auditors have as much technical information as possible (architecture, source code, telephone contacts, identifiers, etc.) before starting the analysis. They also have access to technical contacts related to the target** |  |
|  | **v. if the applicant uses and/or develops smart-contracts, a cybersecurity source code review of them** |  |
| **C** | **Description of conducted audits of the ICT systems including used DLT infrastructure and security arrangements** |  |
| **D** | **Description of the relevant information set out in subparagraphs a) and b) in non-technical language of the information provided under points a) and b).** |  |
| **E** | **DORA Regulation (EU) 2022/2554 Roadmap** | *Please provide a roadmap to your notification in which you provide insight into the steps your company is taking to be DORA-compliant in a timely manner. We expect this roadmap to provide clear insight into when policies and procedures are (finally) drawn up and when they are implemented within the organization, including any intermediate steps.* |

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

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

|  |  |  |
| --- | --- | --- |
| **A** | **How the notifying entity ensures that:** | *Please note that the AFM has published FAQs on their website on asset segregation. We expect you to take available supervisory guidance into account when filling in this form.* |
|  | **i. clients’ funds are not used for its own account** |  |
|  | **ii. crypto-assets belonging to the clients are not used for its own account** |  |
|  | **iii. the wallets holding clients’ crypto-assets are different from the notifying entity’s own wallets** |  |
| **B** | **Detailed description of the approval system for cryptographic keys and safeguarding of cryptographic keys (for instance, multi-signature wallets)** |  |
| **C** | **How the notifying entity segregates clients’ crypto-assets, including from other clients’ crypto-assets in the event of wallets containing crypto-assets of more than one client (omnibus accounts)** |  |
| **D** | **Description of the procedure to ensure that clients’ funds (other than e-money tokens) are deposited with a central bank or a credit institution by the end of the business day following the day on which they were received and are held in an account separately identifiable from any accounts used to hold funds belonging to the notifying entity** | *Please also include information regarding which bank accounts are used, including bank accounts in the Union where client funds are deposited or will be deposited.* |
| **E** | **Where the notifying entity does not intend to deposit funds with the relevant central bank, which factors the notifying entity is taking into account to select the credit institutions to deposit clients’ funds, including the notifying entity’s diversification policy, where available, and the frequency of review of the selection of credit institutions to deposit clients’ funds** |  |
| **F** | **How the notifying entity ensures that clients are informed in clear, concise and non-technical language about the key aspects of the notifying entity’s systems and policies and procedures to comply with Article 70(1), (2) and (3) of Regulation (EU) 2023/1114** |  |

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

## **Custody and administration policy**

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

|  |  |  |
| --- | --- | --- |
| **A** | **Description of the arrangements linked to the type or types of custody offered to clients, a copy of the notifying entity’s standard agreement for the custody and administration of crypto-assets on behalf of clients as well as a copy of the summary of the custody policy made available to clients in accordance with Article 75(3) of Regulation (EU) 2023/1114** |  |
| **B** | **Notifying entity’s custody and administration policy, including a description of identified sources of operational and ICT risks for the safekeeping and control of the crypto-assets or the means of access to the crypto-assets of clients, together with:** |  |
|  | **i. the policies and procedures, and a description of, the arrangements to ensure compliance with Article 75(8) of Regulation (EU) 2023/1114** |  |
|  | **ii the policies and procedures, and a description of the systems and controls, to manage those risks, including when the custody and administration of crypto-assets on behalf of clients is outsourced to a third party** |  |
|  | **Iii. the policies and procedures relating to, and a description of, the systems to ensure the exercise of the rights attached to the crypto-assets by the clients** |  |
|  | **iv. the policies and procedures relating to, and a description of, the systems to ensure the return of crypto-assets or the means of access to the clients** |  |
| **C** | **Information on how the crypto-assets and the means of access to the crypto-assets of the clients are identified** |  |
| **D** | **Information on arrangements to minimise the risk of loss of crypto-assets or of means of access to crypto-assets** |  |
| **E** | **Where the crypto-asset service provider has delegated the provision of custody and** **administration of crypto-assets on behalf of clients to a third-party:** |  |
|  | **i. information on the identity of any third-party providing the service of custody and administration of crypto-assets and its status in accordance with Article 59 or Article 60 of Regulation (EU) 2023/1114** |  |
|  | **ii. description of any functions relating to the custody and administration of crypto-assets delegated by the crypto-asset service provider, the list of any delegates and sub-delegates (as applicable) and any conflicts of interest that may arise from such a delegation** |  |
|  | **iii. description of how the notifying entity intends to supervise the delegations or sub-delegation** |  |

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

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

|  |  |  |
| --- | --- | --- |
| **A** | **Rules regarding the admission of crypto-assets to trading** |  |
| **B** | **Approval process for admitting crypto-assets to trading, including the customer due diligence carried out in accordance with Directive (EU) 2015/849** |  |
| **C** | **List of any categories of crypto-assets that will not be admitted to trading and the description of the reasons for such exclusion** |  |
| **D** | **Policies and procedures and fees for the admission to trading, together with a description, where relevant, of membership, rebates and the related conditions** |  |
| **E** | **Rules governing order execution, including any cancellation procedures for** **executed orders and for disclosing such information to market participants** |  |
| **F** | **Policies and procedures adopted to assess the suitability of crypto-assets in accordance with Article 76(2) of Regulation (EU) 2023/1114** |  |
| **G** | **Systems, procedures and arrangement put in place to comply with Article 76(7) points (a) to (h) of Regulation (EU) 2023/1114** |  |
| **H** | **Systems, procedures and arrangements to make public any bid and ask prices, the depth of trading interests at those prices which are advertised for crypto-assets through their trading platforms and price, volume and time of transactions executed in respect of crypto-assets traded on their trading platforms** | *Please include information if you make use of third-party services such as a price oracle, to establish the price.* |
| **I** | **Fee structures and a justification of how they comply with the requirements laid down in Article 76(13) of Regulation (EU) 2023/1114** |  |
| **J** | **Systems, procedures, and arrangement to keep data relating to all orders at the disposal of the competent authority or the mechanism to ensure that the competent authority has access to the order book and any other trading system** | *Please include clear evidence (e.g., mapping table) that you obtain and hold at least the records that are included in the tables of the MiCAR RTS specifying the content and format of order book records for CASPs operating a trading platform for crypto-assets (see tables 2 and 3 of the Annex).* |
| **K** | **With regards to the settlement of transactions:****i. whether the final settlement of transactions is initiated on the distributed ledger or outside the distributed ledger** |  |
|  | **ii. Timeframe within which the final settlement of crypto-asset transactions is initiated** |  |
|  | **iii. Systems and procedures to verify the availability of funds and crypto-assets** |  |
|  | **iv. Procedures to confirm the relevant details of transactions** |  |
|  | **v. Measures foreseen to limit settlement fails** |  |
|  | **vi. Definition of the moment at which settlement is final and the moment at which final settlement is initiated following the execution of the transaction** |  |
| **L** | **Policies and procedures and systems to detect and prevent market abuse, including information on the communications to the competent authority of possible market abuse cases** | *Please also include a description of any alerting or market monitoring software used to detect market abuse.* |

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

|  |
| --- |
|  |

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

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

|  |  |  |
| --- | --- | --- |
| **A** | **Description of the commercial policy established in accordance with Article 77(1) of Regulation (EU) 2023/1114** |  |
| **B** | **Methodology for determining the price of the crypto-assets that the notifying entity proposes to exchange for funds or other crypto-assets in accordance with Article 77(2) of Regulation (EU) 2023/1114, including how the volume and market volatility of crypto-assets impact the pricing mechanism** | *Please include information if you make use of third-party services such as a price oracle, to establish the price.* |

## **Execution policy**

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

|  |  |  |
| --- | --- | --- |
| **A** | **Arrangements to ensure the client has provided consent on the execution policy prior to the execution of the order** |  |
| **B** | **List of the trading platforms for crypto-assets on which the notifying entity will rely for the execution of orders and the criteria for the assessment of execution venues included in the execution policy in accordance with Article 78(6) of Regulation (EU) 2023/1114** |  |
| **C** | **Which trading platforms it intends to use for each type of crypto-assets and confirmation that it will not receive any form of remuneration, discount or non-monetary benefit in return for routing orders received to a particular trading platform for crypto-assets** |  |
| **D** | **How the execution factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-assets or any other relevant factors are considered as part of all necessary steps to obtain the best possible result for the client** |  |
| **E** | **Where applicable, the arrangements for informing clients that the notifying entity will execute orders outside a trading platform and how the notifying entity will obtain the prior express client consent before executing such orders** |  |
| **F** | **How the client is warned that any specific instructions from a client may prevent the notifying entity from taking the steps that it has designed and implemented in its execution policy to obtain the best possible result for the execution of those orders in respect of the elements covered by those instructions** |  |
| **G** | **Selection process for trading venues, execution strategies employed, the procedures and processes used to analyse the quality of execution obtained and how the notifying entity monitors and verifies that the best possible results were obtained for clients** |  |
| **H** | **Arrangements to prevent the misuse of any information relating to clients’ orders by the employees of the notifying entity** |  |
| **I** | **Arrangements and procedures for how the notifying entity will disclose to client’s information on its order execution policy and notify them of any material changes to their order execution policy** |  |
| **J** | **Arrangements to demonstrate compliance with Article 78 of Regulation (EU) 2023/1114 to the competent authority, upon the request of the** **authority** |  |

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

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

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

## **Transfer services**

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

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

**Additional information:**

1. **Cross-border provision of crypto-asset services** (as meant under Article 65 MiCAR)

Do you intend to provide crypto-asset services in other EU Member States than the Netherlands?

* Yes, then please provide the following information
* No

|  |  |  |
| --- | --- | --- |
| **A** | **List of the Member States in which the crypto-asset service provider intends to provide crypto-asset services** |  |
| **B** | **The crypto-asset services that the crypto-asset service provider intends to provide on a cross-border basis** |  |
| **C** | **Starting date of the intended provision of the crypto-asset services** |  |
| **D** | **List of all other activities provided by the crypto-asset service provider not covered by MiCAR** |  |

1. **Orderly wind-down of crypto-asset service providers** (as meant under Article 74 MiCAR)

Crypto-asset service providers that provide the services referred to in Articles 75 to 79 shall have in place a plan that is appropriate to support an orderly wind-down of their activities under applicable national law, including the continuity or recovery of any critical activities performed by those service providers. That plan shall demonstrate the ability of crypto-asset service providers to carry out an orderly wind-down without causing undue economic harm to their clients.

|  |
| --- |
| *Please note that an orderly wind-down plan describes the process where the company is no longer viable and is compelled to wind down. Scenarios where the business exit is done as a strategic decision (e.g., sale of the business) do not cover wind-down planning.**We expect at least the following elements to be included in the orderly wind-down plan:** *Organizational descriptions, financial statements and projections*
* *Clearly specified roles and responsibilities*
* *Identification of wind down scenarios*
* *Impact assessment (on consumers, counterparties, other stakeholders)*
* *Operational analysis of wind-down procedures (incl. action plan regarding the operational processes to be followed during the wind-down process)*
 |

1. Please note that this notification form is based on a draft version of the regulatory technical standards (RTS) specifying the information to be included in an application for authorisation as crypto-asset service provider (see Article 60(13)) and may be subject to change, meaning that the AFM may request the notifying party to supplement and/or adjust the required information. The latest version of the draft RTS can be found on the website of ESMA. [↑](#footnote-ref-2)