| Reply form  to the Consultation Paper on certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience – third consultation paper |
| --- |
|  |

## 

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper and in particular on the specific questions. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **25 June 2024.**

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Use this form and send your responses in Word format (**pdf documents will not be considered except for annexes**);
3. Please do not remove tags of the type <ESMA\_QUESTION \_MIC4\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
4. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
5. When you have drafted your response, name your response form according to the following convention: ESMA\_MIC4\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_MIC4\_ABCD\_RESPONSEFORM.
6. Upload the form containing your responses, **in Word format**, to ESMA’s website (www.esma.europa.eu under the heading “Your input – Open Consultations” -> Consultation Paper on guidelines on conditions and criteria for the classification of crypto-assets as financial instruments”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

# All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites crypto-assets issuers, crypto-asset service providers and financial entities dealing with crypto-assets as well as all stakeholders that have an interest in crypto-assets.

**General information about respondent**

| Name of the company / organisation | Bitpanda GmbH |
| --- | --- |
| Activity | Crypto Broker |
| Are you representing an association? | ☐ No |
| Country/Region | Austria |

**Questions**

1. **Do you agree with ESMA’s analysis on the personal scope of Article 92 of MiCA? Are there other types of entities in the crypto-asset markets that should be considered as a PPAET (e.g. miners/validators)? Do you believe that CASPs providing custody and administration of crypto-assets on behalf of clients should also be considered as PPAETs for the purpose of this RTS? Please elaborate.**

<ESMA\_QUESTION\_MIC4\_1>

**Bitpanda Answer:**

***Scope of Article 92***

* In general, we agree with the approach that requirements shall be based on similar requirements to Regulation (EU) No 596/2014 (MAR) and Regulation (EU) 2016/ 957 (CDR). Therefore, the scope of persons that would be considered as PPAET in the draft RTS should closely follow the scope and spirit of MiCA. This means we should not expand the scope of PPAETs for the crypto-assets sector - which, we believe, is the case in the present draft. If we are saying that we are taking the same approach as for the financial sector, then, trading platforms shall be the main persons who are subject to the requirements (i.e. main PPAETs).
* In our view the scope of persons is too broadly constructed in the draft RTS and goes beyond the provisions of MiCA. Article 92(1) of MiCA refers to “person professionally arranging or executing transactions in crypto-assets”. MiCA does not provide a definition of such persons and does not provide further explanation in the recitals.
* The definition in point 28 of Article 3(1) of MAR defines such persons “as a person professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments”. Therefore the scope of persons under MAR is understood quite narrowly and covers only two MiFID services - reception and transmission of orders and execution of orders.
* Recital 2 of ESMA draft RTS on arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-assets states that such persons shall include Crypto-Asset Service Providers (CASPs) operating a trading platform, providing the reception or transmission of orders for crypto-assets on behalf of clients, the execution of orders for crypto-assets on behalf of clients, providing portfolio management of crypto-assets, providing exchange of crypto assets for funds or exchange of crypto-assets for other crypto assets. Therefore, the scope of persons subject to market abuse requirements would be extended even if it was not the intention of co-legislators of MiCA. It is unclear why under MiFID certain persons are not included (i.e. persons dealing on their own account, portfolio managers) and under MiCA they are included in the scope of persons subject to market abuse arrangements requirements. This is especially relevant taking into account that the drafting of the relevant provisions of regulation and the essence of the services are almost identical. From a practical perspective, cases where portfolio managers, persons who provide exchange of funds to crypto-assets or other crypto-assets engage into market manipulation would be limited and no practical examples could be identified under current market abuse practice.
* Another element is regarding miners and validators. They should be considered for the purpose of market abuse requirements in general (i.e. for the purpose of Article 91). However, they should not be considered for the scope of Article 92 since they are not persons professionally arranging or executing transactions - this term is understood in a limited scope under MiCA (persons who provide crypto-asset services only). And other MiCA requirements do not apply for persons who are not CASPs. By adding validators and miners in the scope of PPAET, persons who only process transactions would be captured even if they do not act in a regulated crypto assets industry: in other words we believe this is an unsubstantiated extension of the scope of MiCA.
* Generally we want to highlight that also CASPs should not be responsible for detecting market abuse in mining or validation of transactions, unless they themselves interact with the transactions (e.g. are mining themselves or are at least involved in the transaction). A general obligation to review DLT-based transactions would not only be a strong burden for the CASPs, but would also go way beyond the scope of Art. 92 MiCAR. As the obligations in this regard lack legal clarity, we ask ESMA to state more precisely in which - rare - cases CASPs need to analyse DLT transactions for market abuse reasons and to further describe the scope of this obligation - if at all - in more concrete matters.

***Scope of admission to trading***

* In our view the draft RTS could clarify the scope of the term “admitted to trading” that is referred to in Article 86 of MiCA since this definition is a key term because it covers all Title VI of MiCA. At the moment it is not clear if Title VI of MiCA will apply only where crypto assets are listed on a trading platform in the EU or in any jurisdiction.
* The issue is that some crypto assets cannot be admitted to trading in the EU trading platform but are able to be bought by EU clients via crypto-asset exchanges (CASPs providing crypto-asset service referred to in point c or d of Article 3(16) of MiCA). Such cases are possible crypto-asset exchanges buying crypto-assets on their own account and then clients can purchase in the EU where white paper of the issuer is available. In such a case, that is described above, it is not clear if Title VI applies.

***On chain data***

* We would also like to point out that any requirements to analyse and provide on-chain data for blockchain and transaction in general should be limited to the overall description and preliminary analysis. Furthermore it needs to be clarified what the scope of this analysis is - from our point of view it needs to be restricted to transactions where the CASP was involved (e.g. as party, validator or miner). Otherwise, this obligation would be limitless and, it is impossible to analyse the whole on-chain conduct given the size of the network and numerous projects. Therefore, this should be strictly limited.

***Maximum extractable value (MEV)***

* Furthermore, we would like to flag the problem of MEV, where ESMA took a prohibitive approach suggesting that MEV may suggest the existence of market abuse and therefore, eligible crypto firms would have to detect and report MEV as STORs. We agree on the points made in ESMA assessment regarding the controversial nature of MEV that can, in certain constellations, act manipulatively and be used to make unfair profits, and in which case should not be allowed. On the other hand, qualifying MEV as market abuse can go beyond the scope of MiCA Article 91 and 92 execution of transaction. Generally speaking, we need to approach this topic with caution and nuanced analysis.
* MEV stands for Maximal Extractable Value. In fact, it is an umbrella term for different actions/characteristics. Therefore, we need to specify the scope/type; otherwise, we risk confusion and generalisation. Associated with MEV is the practice of (i) front-running or (ii) sandwich attacks or (iii) backrunning (IOSCO in 04/2023 provided a report on Defi where it addressed the issue). Those techniques can be used by validators and block proposers in order to re-order (re-position, sequencing) transactions. This then allows them to bring out profits by targeting the maximal allowable slippage for on-chain transactions. In this context, CASPs are not able to prevent or detect MEV since they are, predominantly, not involved in this level of transaction.
* Accordingly, in terms of scope, it is not clear for us at all what the role of CASPs in the context of MEV should be. We therefore suggest, if any, to include the obligation to monitor for MEV, in the cases of CASPs, only if they are involved in the transaction (see the above points, eg., as a miner, party or validator) - however, even here it would not be straightforward and much limited, or not really viable due to Proposer-Builder Separation (PBS) nature. We need to highlight that it cannot be the role of CASPs to monitor the whole market for potential market abuse cases. Art. 92 MiCA clearly implies that the scope of this obligation only includes transactions where the CASP is involved. We therefore strongly urge that ESMA clarifies the scope of the obligation regarding “monitoring of DLT-based transactions”. In other words, the monitoring of potential breaches of market abuse rules by miners and/or validators should not be within the scope of CASP obligations, unless the CASP is directly involved in such a transaction.
* We would like to further encourage to see both sides of the coin here, as the topic is not as straightforward as it may appear to be, especially given the more positive and useful operational side. What is more, such an approach based on a case-by-case analysis will help to maintain competitiveness of the EU worldwide (there is a risk of firms and users moving outside the EU given, the preliminary proposed prohibitive stance) and, rightfully, falls under the proportionality principle and tech-agnostic approach.
* Therefore, we believe that it will be proportionate to set a limit and direction when MEV may be considered as abusive and when not. A good example here is the recent indictment of the Department of Justice in the US, where it appears to take the approach of demarcating a line between MEV practices and exploitations.
* The following are some of examples of when MEV is prohibitive (again, case-by-case analyse with context and facts needs to be undertaken):
  + false signatures and exploiting a flaw in MEV-boost to illicitly benefit from reordering transactions
  + frontrunning, sandwich attack or back running
  + creating higher gas fees and congestion due to manipulation
* In contrast, some examples of more ethical usage of MEV that is beneficial for the crypto industry are amongst others:
  + improves blockchain network efficiency
  + can increase the network security (competition for validators and miners)
  + swift liquidations ensuring that lenders are paid back (avoidance of negative-depth)
  + participants are able to use arbitrage opportunities
  + ensures accurate DEX pricing
* Importantly to note, MEV could be mitigated by technologies seeking to minimise opportunity of MEV or make it more democratised (currently, various solutions are being used, further developed and improved or being more investigated given the controversy of the topic):
  + the design of the trading mechanism
  + usage and further development of “proposer-builder separation” (PBS)
  + fair sequencing services
  + off-chain transactions and batching
  + flashbots reducing impact of MEV
  + introduction of MEV auctions (auctions to bid over transaction prioritisation)
* Finally, we would like to highlight that today’s MEV might not look like tomorrow’s MEV - the dynamic is high and alterable. There is still ongoing research on how to architect the block-building process ([See source](https://writings.flashbots.net/the-future-of-mev-is-suave)) of the most mature network (where most of the MEV happens), which deals precisely with this issue (how to avoid exploitation but in a decentralised way). Therefore, it is important to put MEV against that backdrop and consider the above-mentioned aspect on a case-by-case basis, which only illustrates how dynamic and diversified the space is expanding beyond the current frameworks. Based on this, we would like to, once again, reiterate that CASPs should not be charged here with monitoring and detection as explained above.

***Coordination procedures between competent authorities for detection and sanctioning of cross-border market abuse***

* We welcome ESMA's position concerning not being overly prescriptive (definition of crossborder market abuse situation is broad and encompasses various misconducts) in defining abuses. We find it very relevant to give however more examples (non-exhaustive) what crossborder market abuse situations are and what they entail.
* We agree that ESMA should take the lead role in coordinating the investigation or enforcement activities started by two or more competent authorities, when requested by any of them (point 31). We also welcome that an NCA receiving information on a market abuse case, which may fall outside of its area of competence, can simply forward that information to the potentially relevant NCA(s).

<ESMA\_QUESTION\_MIC4\_1>

1. **Do you agree with the proposed elements that should constitute appropriate arrangements, systems and procedures to detect and prevent market abuse? If not, please specify the article of the draft RTS and elaborate.**

<ESMA\_QUESTION\_MIC4\_2>

**Bitpanda Answer:**

* We welcome the position that systems, arrangements, and procedures should be developed around the principle of proportionality in relation to size and nature of business activity and the risk that these activities pose to the market. We would propose to add an addition of “Market Abuse” to the sentence: “*adequately prevent and detect any suspicious activity* concerning Market Abuse a*nd to report it to the relevant NCA in a timely fashion*”. This will reflect the nature of this requirement better, since ESMA also considers certain actions falling outside the scope of market abuse.
* We do not believe however that Article 2 (b) is proportionate (and other ones that cite similar). It also creates uncertainty in terms of its very broad scope. This Article says that:
  + *effective and ongoing monitoring, for the purposes of detecting and identifying other aspects of the functioning of the distributed ledger technology, such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed*
* We would like to flag that we need to make it clear that subjects of the Market Abuse rules cannot be charged with monitoring, detection and identification of the whole blockchain activities. This would be disproportionate and out of scope given the significant size of the blockchain itself. A monitoring of the on-chain transactions of orders after they leave the ecosystem of the executing entity, shall not apply. The activities of concerned crypto firms are mostly off-chain and CASPs are in most cases only recipients of DLT-transactions. We agree that the scope can be broadened only in the following cases (see also above): a) the CASP is acting as miner or b) as validator, c) the CASP is directly involved in the transaction (sender, recipient or similar) or d) the transaction itself involves directly DLT-transactions (e.g. DEX, settlement via DLT etc etc). It should therefore be clarified that, in all other cases, CASPs should not be responsible for monitoring DLT-transactions, as they have no connection to the CASP whatsoever.
* In addition, it is not clear if we are considering internal or external audits (Art. 3(2b)) - another point that needs clarification. From proportionality arguments and as MiCAR itself does not contain obligations for audits. Thus, we strongly urge for a more flexible approach, e.g. audit by Compliance or in any case internal.

<ESMA\_QUESTION\_MIC4\_2>

1. **Do you agree with the proposed STOR template as presented in the Annex of the RTS?**

<ESMA\_QUESTION\_MIC4\_3>

**Bitpanda Answer:**

* We agree with the template of STOR. However, considering the information it requires it is clear that certain entities (such as exchanges, portfolio managers) will not have the information that is required under this template (such as type of trading activity, trading platform where order was placed or the transaction was executed). To this, it should be explicitly clarified by ESMA that a "best effort approach" is sufficient for filling out the template.
* Next, given the short time frame to file a STOR, CASPs should have more flexibility to not to include certain items. This should be mentioned explicitly in the RTS. In the template - e.g. where specific technical information is required (ISO, MIC, LEI, Personal Identifier etc) it should be clarified that CASP could send the STOR without such information and/or that they can file this information at a later stage.
* Lastly, we however do not agree that the description of DLT ledger shall be included. This is too technical and in other sectors technical details are not required. If any, this should be strictly minimised to the simple information about the type of DLT/blockchain network (eg., name).

<ESMA\_QUESTION\_MIC4\_3>

1. **Is there any parameter or naming convention that in your view should be modified to facilitate the identification of suspicious orders/transactions/behaviours involving crypto-assets?**

<ESMA\_QUESTION\_MIC4\_4>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_4>

1. **In Section II of the Annex, would the concept of ‘location’ be applicable to a distributed ledger? For instance, would the IP address of miners/validator nodes in the network be useful in a context where it can be masked through VPNs?**

<ESMA\_QUESTION\_MIC4\_5>

**Bitpanda Answer:**

* With regards to DLT, we think that the concept of location does not make sense because the origin of a transaction (tx) is not known to any other node than the originating one. The miners that pick it up could be identified by their voluntarily given records, but that does not make sense in our opinion - because they just validate a tx and not created it. Next, it only makes sense for CASP if they can identify one party (say a user who receives a suspicious deposit) with their location, but for the tx itself, we do not see the location having any relevance. As stated above several times, CASPs should only be obligated to monitor in any case if they are involved in the DLT-transaction.
* We think that the location in the context of crypto tx is the network; for instance: suspicious tx1, location: Tron network, time: see timestamp
* Furthermore, given the inherent transparency of the blockchain transaction, localisation data incl. miners/validator IP should be eased in the template. Instead, we should provide the basic data and point of reference that can be then searched in blockchain explorer and blockchain forensic tools. Therefore, the collection of the proposed information would not benefit the overall compilation of STOR but will add to already extensive reporting and data collection requirements.
* Finally, the amount of specific individual data to be collected should be also assessed against the requirements of GDPR and usefulness in terms of reporting and investigative measures.

<ESMA\_QUESTION\_MIC4\_5>

1. **Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.**

<ESMA\_QUESTION\_MIC4\_6>

**Bitpanda Answer:**

* From our point of view, the template seems complete, even overloaded with information that puts into question its relevance (as mentioned above). Certain sections/elements should be streamlined and the information requirement lessen (See Q3, Q5 above).

<ESMA\_QUESTION\_MIC4\_6>

1. **Please provide information about the estimated costs and benefits of the proposed technical standard, in particular in relation to the arrangements, systems and procedures to prevent and detect market abuse.**

<ESMA\_QUESTION\_MIC4\_7>

**Bitpanda Answer:**

* The rules on Market Abuse and detection will significantly increase the cost of compliance. First of all, the software tools are still developing and adjusting for the crypto specific needs. Currently, third party solutions may cost approximately between 110.000€ - 130.000€ per year or more. In addition to the cost of the software, the internal adjustment will need to take place to accommodate the new requirements which by itself increased the cost. For instance, additional new FTEs will need to be considered and at least another one allocated for alerts handling.
* In this case, we want to highlight that many transactions will involve different CASPs. E.g. User Z goes to CASP A for advice or portfolio management, gives the order (RTO service) to CASP B, who forwards it to CASP C (Exchange), which hedges itself (that is buy or sell crypto assets on its own account) at CASP D (Trading Platform). Therefore, from our perspective it would seem fine if only trading platforms would need to have a tool at hand, while other CASPs - also from a proportionality approach - could also fulfil the obligation by taking samples and similar procedures. Such an approach should be clarified in the RTS itself.

<ESMA\_QUESTION\_MIC4\_7>

1. **Do you agree with ESMA’s approach regarding consistency between the MiCA and MiFID II suitability regimes? If you think that the two regimes should diverge, where and for which reasons?**

<ESMA\_QUESTION\_MIC4\_8>

**Bitpanda Answer:**

* We disagree that those Guidelines require the same level of suitability assessment as for the financial instruments which could include various instruments (i.e. bonds and common shares have different nature and investors seek different objectives choosing one or other), meanwhile the suitability assessment for crypto assets are based on one class of asset – crypto-assets, so it shall not take into account other instruments (such as financial instruments). If financial instruments are supposed to be taken into account, then it is the provision of MIFID investment advice or portfolio management.
* Suitability assessment for a certain type of crypto-assets should indicate that crypto assets vary significantly based on their type and characteristics - whether it is stablecoins or other crypto assets. Meanwhile different crypto-assets in general (e.g. Bitcoin vs Meme Coin), should indicate that crypto assets vary significantly based on clients' purposes. Therefore, the granularity of suitability assessment cannot be the same as for MIFID’s assessment (as pointed out above: different levels of elements that are taken into account, data available etc. See also below the next point).
* Importantly, the market and investment concept is also different since it covers only one type of asset class. The elements that differ and are particular for the crypto-assets are amongst others: (a) market dynamics, (b) specific types of crypto-assets categories (incl. their use-cases, inherent features and concepts), (c) still more volatile nature, (d) data availability and level of granularity and, (e) changing regulatory developments.

<ESMA\_QUESTION\_MIC4\_8>

1. **Do you think that the draft guidelines should be amended to better fit crypto-assets and the relevant crypto-asset services? In which regard? Please justify your answer.**

<ESMA\_QUESTION\_MIC4\_9>

**Bitpanda Answer:**

* In our view, Guidelines should address the specific nature of the crypto assets market and that advice or portfolio management on crypto assets are much narrower than those services would be provided for the financial instruments.
  + CASP would not have capabilities, experience, resources (i.e. portfolio managers, research) to provide advice or portfolio management taking into account overall clients portfolio (i.e. which include financial instruments).
  + Advice and portfolio management guidelines need to acknowledge the unique nature of the crypto industry and different crypto-assets. Although fundamental and technical analysis applies, the scope and extent will be different including market dynamics.
  + The service is newly regulated under MiCAR - experience and set-up is therefore not existing. It should be clarified that a more proportional approach is taken (e.g. regarding experience of Management Board and/or of advisors/portfolio managers)
* It needs to be understood that Advice/Portfolio Management for Cryptos will - different as for financial instruments, where often the whole portfolio is taken into account - only be based on a smaller part of the portfolio. It seems not adequate to oblige CASPs to analyse the whole portfolio and take the overall allocation into account - if the service is only used for a part of the clients portfolio. Thus, there should be no need to assess such information and give sensitive personal information (financial information of a client), which will not be used.
* Furthermore, we would like to point out that we do not agree with the general approach proposed in point 39 (“*For such risky and complex products as crypto-assets, crypto-asset service providers should collect more in-depth information about the client than they would collect when less complex or risky products are at stake*.”). We strongly urge here that ESMA differentiates between different types of crypto-assets (e.g. ARTs, EMTs, Bitcoin vs MemeCoins etc) or to avoid such generic statements and the sweeping “condemnation” of an established Asset-class.

<ESMA\_QUESTION\_MIC4\_9>

1. **Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?**

<ESMA\_QUESTION\_MIC4\_10>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_10>

1. **Do you agree with the approach taken by ESMA in the draft guidelines for crypto-asset service providers providing transfer services for crypto-assets on behalf of clients as regards procedures and policies, including the rights of clients? Please also state the reasons for your answer.**

<ESMA\_QUESTION\_MIC4\_11>

**Bitpanda Answer:**

* To start, we would like to comment on the scope of this service. We believe that the scope of this service is unclear. Definition is broad, however, not all services should be seen as transfer of service from one DLT to another, especially if they are connected to underlying service (for example such as withdrawals, transfer without change of legal ownership) unlike the standalone transfer. We also believe that we need to specify on-chain vs off-chain transfer incl. internal transfer in CASPs ecosystem. We urge here to provide further clarification as to the scope, when essentially the transfer of service is triggered. Furthermore it needs to be clarified how - if at all - Transfer Services overlap with PSD II.
* We would like to further observe that, already now, the user is provided with comprehensive information concerning the transfer that, in our opinion, is sufficient. The information is, additionally, already available on the blockchain and it seems therefore overly burdensome to oblige CASPs for such a “duplication”. For example the following information is already provided:
  + type of network, ID of transaction, type, date, status, fee, total amount.
* We find the requirement of “durable medium” and information when the transaction is irreversible is not necessary and excessive. With regards to “durable medium”, Art. 82 of MiCA does not require even a contract to be in that format. Moreover, CASPs would have more flexibility in providing the information and, certainly, would positively impact internal operations and processes. Also, there are no material impairments for the users here. We should therefore have more flexibility as to the format, e.g. pop-up, information in the order confirmation etc. Especially with the time frame of the proposed Guidelines (between finalisation and execution) this would otherwise not be feasible.
* With regards to the time of irreversibility, it is vital to note that confirmation depends on the network itself. Sometimes 1 confirmation is considered irreversible (e.g. IOTA network), sometimes more confirmations are needed (e.g. 3 for Bitcoin). This varies heavily between blockchains and is in most cases a “best effort analysis”, without a fixed and aligned approach within the industry. So the important element is that this is not a set-in-stone number. In addition, there may be times that average confirmation takes more due to increased traffic. For example:
  + *“Bitcoin transactions are generally considered completed once they have been confirmed in 1-6 blocks. As each block on average takes 10 minutes to be confirmed into a new block by the* [*Bitcoin Mining*](https://www.athena-alpha.com/what-is-bitcoin-mining/) *process, this means your transaction will take anywhere from 0-60 minutes on average to be completed”* (See [source](https://support.nexo.com/article/processing-time-of-cryptocurrency-deposits-blockchain-confirmations))
  + *“Each block is mined at a different rate, depending on the blockchain. For example, on the Bitcoin blockchain, a block is mined on average every 10 minutes, and Nexo only credits Bitcoin top-ups to a client’s account after a minimum of 3 confirmations, which takes approximately 30 minutes. However, sometimes when the network is heavily used, it can take Bitcoin miners 30 or even 60 minutes to mine a single block (1 confirmation)”* (See [source](https://www.athena-alpha.com/how-to-confirm-a-bitcoin-transaction/#:~:text=Bitcoin%20transactions%20are%20generally%20considered,on%20average%20to%20be%20completed.))
* Therefore, even if there is a standard, usual time for confirming a transaction, this may not be the case. Instead of giving a precise time, we would strongly suggest opting for ranges and additional communication that informs clients and urges them to double check addresses, to first send a test transaction to a familiar wallet with a smaller amount. With this approach we educate investors rather than giving them exact time that may make them feel at ease while then the confirmation was longer or shorter.
* Another point that we would like to raise is recital 16. We find it very strange to do that between receipt, but before the execution. This is because the timing of this occurs, more or less, in the same second; that is, it is fully automated. We believe, therefore, that it should be clarified that this is allowed at least WITHIN the process and therefore before final execution. In practice, the clients will be informed by a pop up window and will have to give its final consent and confirmation within the process of the transfer but before the final green lighting of the transfer.
* Furthermore, we believe that recitals 17 and 18 should be clarified. It shall be clarified that TOFR is also possible at the same time and also that an adequate amount of time (e.g. on the same day; within the same hour) should be seen as adequate. These recitals should not require a “holding” of a transaction. Furthermore, we are of the opinion that recitals 17 and 18 seem to be redundant as the wording is nearly identical. In the case ESMA wants to address different topics in Recital 17 and 18 we ask for clarification within the guidelines.
* Next and final, we believe that recital 21 is odd in the sense of potential confusion and inconsistency. Did ESMA mean recital 19 instead of 16? Additionally, the warning and the charges should be in the acceptance flow (see point on information before the execution) and not on durable medium (both for recital 19 and 16).
* Overall, we understand the goal of the guidelines but urge for a) more clarity regarding the scope of transfer services - especially when to apply those information requirements, b) for a more flexible approach (e.g. no durable medium requirement, already within the order flow instead of “between finalisation and execution”) as well as c) generally for a review of the - very broad - information requirements. From our point it seems that the information requirements go way beyond the generic points in Art 82 MiCAR and we ask ESMA to consider reducing them.

<ESMA\_QUESTION\_MIC4\_11>

1. **Do you think that the draft guidelines address sufficiently the risks for clients related to on- and off-DLT crypto-asset transfers? Please justify your answer.**

<ESMA\_QUESTION\_MIC4\_12>

**Bitpanda Answer:**

* Yes, we believe that diversified information required sufficiently addresses the risk but we need to strengthen education here - especially in the context of the irreversibility of transactions as explained above. Otherwise, we continue to lack financial education likewise the mentality to conduct “one’s own research” (do your own research rule). On top, we apply excessive obligations on CASPs that, ultimately, will not serve as customer protection (as explained above in Q.11).
  + Important to mention, it is industry best practice to have already now user friendly and sufficiently transparent processes and procedures. And equip investors with the necessary information. Any additional inquiries can be addressed with the customer support service and through crypto academies for self-education.
* As mentioned above, we believe that the information requirements in the proposed guidelines might be considerably too excessive. We therefore would like to generally ask for a review of the - very broad - information requirements. From our point it seems that the information requirements go way beyond the generic points in Art. 82 MiCAR and we ask ESMA to consider reducing them.

<ESMA\_QUESTION\_MIC4\_12>

1. **Are there any additional comments that you would like to raise and/or information that you would like to provide, for example, on whether other relevant points or clients’ rights should be considered?**

<ESMA\_QUESTION\_MIC4\_13>

**Bitpanda Answer**

* As specified above, the scope of the service should be clarified and described. Furthermore, we would propose to reduce the information requirements (see above) and include e.g. only rights of clients instead of different information obligations.

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_13>

1. **Do you support ESMA’s interpretation of the term, ‘systems’ in the mandate? If not, please explain your understanding of the term (and provide examples if possible).**

<ESMA\_QUESTION\_MIC4\_14>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_14>

1. **Are there other ‘appropriate Union standards’ beyond those identified in the consultation paper that you consider relevant for this mandate? If yes, please list them and provide a rationale for why they would be relevant.**

<ESMA\_QUESTION\_MIC4\_15>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_15>

1. **Do you agree with the inclusion of minimal administrative arrangements in Guideline 2 (i.e., no reference to implementing a risk management framework)? If no, please explain whether you would consider either *fewer* or *more* administrative arrangements appropriate.**

<ESMA\_QUESTION\_MIC4\_16>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_16>

1. **Do you support the inclusion of Guideline 5 on ‘cryptographic key management’? Do you consider cryptographic keys relevant as either a ‘system’ or a ‘security access protocol’? Is this guideline fit for purpose (i.e., can cryptographic keys be ‘replaced’ as implied in paragraph 29 of the draft guidelines)?**

<ESMA\_QUESTION\_MIC4\_17>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_17>