ESMA Guidelines on Market Abuse under the MiCA Regulation

November 2025

On 9 July 2025, ESMA published the Guidelines on supervisory practices to prevent and detect market abuse under the Markets in Crypto Assets Regulation(MiCA)[1], aiming to ensure consistent and uniform supervision by the National Competent Authorities (NCAs) across Member States. These Guidelines complement the Delegated Regulation for reporting suspicious transactions or orders under MiCA[2].

The primary objective of these Guidelines is to establish a consistent approach among NCAs to prevent and detect market abuse under MiCA, specifically involving insider trading, unlawful disclosure of insider information and market manipulation.

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council, of 31 May 2023, on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

[2] Commission Delegated Regulation (EU) 2025/885, of 29 April, 2025 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the arrangements, systems and procedures to prevent, detect and report market abuse, the templates to be used for reporting suspected market abuse, and the coordination procedures between the competent authorities for the detection and sanctioning of market abuse in cross-border market abuse situations.

Pregunta

What are the obligations for National Competent Authorities?

Respuesta

NCAs are required to apply the Guidelines three months after their publication date on ESMA's website.

Within two months of the publication date, NCAs must inform ESMA whether they comply with the Guidelines. If they do not comply, NCAs are obliged to provide the reasons for non-compliance or, where applicable, the date by which they intend to apply the Guidelines.

Pregunta

What is the content of these Guidelines?

Respuesta

ESMA's document contains 12 Guidelines, which can be grouped into two main categories based on the topics addressed:

1. General principles for market abuse supervision, detection and prevention (Guidelines 1 to 7)
2. Guidelines on supervision and compliance (Guidelines 8 to 12)

Pregunta

What are the general principles of market abuse supervision, detection and prevention?

Respuesta

1. **Proportionality.** NCAs shall consider in their supervisory activity the relevance of the activities and services provided by persons and entities in the crypto-asset market, as well as the specific risks that

such activities and services pose to market integrity.

2. **Risk-based and forward-looking approach.** NCAs shall consider potential and emerging risks in order to take swift action and expand or adapt their supervisory strategies accordingly.
3. **Knowledge and gained experience in market abuse.** Before resorting to new supervisory measures, NCAs should first integrate those already in place for the detection and prevention of market abuse in financial instruments. If necessary, such existing measures may then be adapted or expanded. In this way, NCAs would be able to monitor manipulative practices stemming from the specific technology underlying crypto-assets (e.g. abusive maximal extractable value, MEV, practices) or from the way they are offered and evaluated (e.g. token supply manipulation or, for stablecoins, the assessment of the backing assets). In addition, NCAs may consider monitoring social media activity to supervise information posted on crypto-assets or by new profiles that might have access to insider information (e.g. employees of crypto-asset service providers, CASPs, miners or validators, etc.).
4. **EU common supervisory culture.** NCAs will exchange information amongst themselves to ensure a shared understanding of the risks associated with crypto-asset markets. They may also propose initiatives to ESMA to foster market convergence, as well as cooperate and exchange information with other authorities, to the extent possible (e.g. authorities responsible for consumer protection or prevention and detection of money laundering and terrorism financing).
5. **Adequate and specialised resources.** NCAs must have dedicated staff with the appropriate expertise and experience on the subject, the necessary technological tools and a data-driven approach to supervision, rather than relying solely on factual events. NCAs shall also provide ongoing training to the staff involved in the oversight of crypto-asset markets.
6. **Dialogue with stakeholders.** To identify emerging risks and new market abuse strategies, as well as to better understand the technological developments enabling the creation of potential solutions (such as new risk-mitigation tools), NCAs shall engage with stakeholders, experts, academics, public advocacy groups, IT firms, data service providers and those persons to whom tasks related to market abuse prevention and detection have been outsourced.
7. **Initiatives to promote market integrity.** NCAs, whether individually or in collaboration with ESMA or other NCAs, should engage in educational and awareness-raising initiatives about practices that may constitute market abuse and their corresponding penalties; NCAs shall use accessible language for these purposes.

Pregunta

What are the main principles of market abuse supervision, detection and prevention?

Respuesta

1. **Data-driven surveillance.** NCAs may conduct market surveillance in collaboration with other competent authorities or, under their responsibility, by delegation to other authorities or service providers, as appropriate. This surveillance activity shall include publicly available data, regulatory data on orders and transactions obtained from CASPs and, where possible, the reconciliation of on-chain, off-chain, and cross-market data. Based on identified risks, information disclosed on social media, web-based platforms, blogs, newsletters and podcasts may also be considered. For this purpose, NCAs may adopt task automation complemented by human analysis.
2. **Supervision of persons professionally arranging or executing transactions (PPAETs).** NCAs must ensure appropriate mechanisms, systems and procedures to prevent and detect market abuse on an ongoing basis. Supervision should be proportionate to the risk, frequency and relevance of supervised activities, based on the nature of the activities carried out by the PPAET. For example, there should be a distinction between CASPs operating a trading platform and CASPs merely receiving, transmitting, or executing orders on behalf of clients.
3. **Management of suspicious transactions or orders reports.** NCAs should establish internal procedures to effectively analyse suspicious transactions or orders reports received from PPAETs and take appropriate measures, proportional to the threat identified.
4. **ESMA coordination.** NCAs may request ESMA the coordination of inspections or investigations in cross-border cases where more than one NCA is competent, or where uncoordinated action may undermine the outcome of the investigation or create additional burdens for market participants.

5. **Obstacles posed by third countries.** NCAs shall inform ESMA and relevant NCAs where, in the course of their supervisory activities, they identify a CASP whose business model might hinder the supervision of market abuse or detect any obstacles in interactions with third-country competent authorities. In assessing potential obstacles, NCAs shall consider aspects such as: a) the legal context of a third country and the difficulties it may entail; b) the feasibility of exchanging information with the third country; c) the structure of the group to which the entity supervised under MiCA belongs to and the individuals with close links to it; d) the location and activities of entities within the group of the MiCA-supervised entity, as well as the persons closely linked to the entity supervised under MiCA.

Link of Interest:

Guidelines on supervisory practices for competent authorities to prevent and detect market abuse under the Markets in Crypto Assets Regulation (MiCA)

This document is a summary of a document published by ESMA. It does not necessarily reflect CNMV's official position, its managers and directors' or the rest of its staff's on the matters addressed.

This document has been drafted using material downloaded from ESMA's website. ESMA does not endorse this publication and in no way is liable for copyright or other intellectual property rights infringements nor for any damages caused to third parties through this publication.

© CNMV. The contents of this publication may be reproduced, subject to attribution.