



DIRECTIVE 2/2026

Monitoring and Control in Information Exchanges with OMIE

06 – May – 2026



INSTRUCTION 2/2026

Monitoring and Control in Information Exchanges with OMIE

1. PREAMBLE

In the exercise of its functions as market operator, OMIE considered it appropriate to facilitate the exchange of information with agents through standardized message interfaces (APIs) that allow the development of applications capable of interacting with the systems and markets operated by OMIE, thus enabling the exchange of information between remote systems.

Since these interfaces were put into operation and, especially, with the arrival of the Continuous Intraday Market (CM) and trading in quarter-hour periods, a significant increase in transactions and mass access has been observed from applications developed by the agents. This high volume of transmitted and processed data could in the future generate slowdowns or delays in operations, affecting all market agents, including those who do not perform such intensive accesses.

To avoid these possible effects, it is essential that agents make rational and appropriate use of OMIE's platforms, ensuring the proper functioning of their applications, keeping access and operations at reasonable levels, and avoiding mass and repetitive actions that unnecessarily impact performance.

In order to supervise such use and maintain operability, OMIE will establish proportionate control measures aimed exclusively at regulating these actions and improving the functioning of the market. These measures will apply to the development, management, and use of agents' applications at different levels (technical, organizational, and awareness), to prevent incidents that may disrupt the normal course of processes.

Given that overly detailed controls could affect the performance of the monitored systems, a model based on a complementary dual control has been defined: on the one hand, online controls over agents' operations, aimed at limiting the impact of abusive or risky actions and, on the other hand, ex post reviews of application behavior, assessed through predefined indicators, notifying agents and requesting corrective measures if the established thresholds are exceeded.



2. DEVELOPMENT

A. IT communications with OMIE platforms

OMIE makes access to its market platforms available to agents through the following APIs:

- *Access via the Web Services (WS) API.*

WS allows market agents' systems to communicate directly with OMIE's systems, enabling all operations necessary to participate in the Day-Ahead Market (DAM) and Intraday Auction Markets (IDAs), as well as to obtain information related to the Continuous Intraday Market (CM) and the processes associated with the management of guarantees and settlements.

- *Access via the Continuous Intraday Market (CM) API.*

CM API allows market agents' systems to communicate directly with the local trading server (LTS), enabling them to obtain in real time the information associated with the market's operation and to automatically perform CM operations.

Continuous adaptation to changing requirements in the different markets, together with constant advances in the state of the art, requires regular adaptation of these APIs so that they work correctly under new requirements. OMIE will endeavor to maintain continuity and compatibility with previous versions of each API and to provide agents, through the market platforms, with reasonable advance notice of any modification that may affect them, so that they have sufficient time to adapt and test their applications before the new version is put into production.

In order to ensure that all applications developed by agents (both those using the Web Services APIs and those using the CM API) meet minimum functionality and performance standards, such applications must pass an Enablement process before operating in production systems. Since enabled applications may undergo subsequent modifications by agents, agents must inform OMIE, prior to putting them into operation, of any change or new version that may have a significant impact on operational access. Depending on the scope of the changes, a new Enablement process may be required before the new versions are put into operation. Likewise, in the event of changes to OMIE's API, OMIE may also require a new enablement process.

Similarly, any malfunction detected during the use of the application in the production environment may lead to the loss of Enablement, requiring the agent to repeat the process to demonstrate that the incident has been correctly remedied.



Likewise, agents must take part in Enablement confirmation processes when OMIE so requires.

B. Obligations of market agents

Agents must ensure at all times that their access does not unjustifiably introduce a significant load on the system nor affect the proper functioning of the market or OMIE's platforms, adopting all reasonable precautions to that end.

In order to keep market agents informed of any abnormal situations and/or behaviors that must be corrected, agents are required to keep the information and contact details available to OMIE on the Market Website up to date.

Agents must comply with the Terms of Use when accessing OMIE's platforms and must also respect the limits established in the control measures and indicators set out in Annexes I and II. If they receive notices due to exceeding these limits —both at business level (unit capacity, guarantees) and in information requests— applications must adapt their behavior so as not to exceed them again. In particular, information requests must be continuously kept below the limits that apply to them.

I. Terms of Use for access to the Market Website

Access to the Market Website may be via browser or via the WS API. In the latter case, a prior Enablement process will be required for the agent's application that will interact with the production systems.

Market agents are responsible for all access done using the security certificates assigned to their company personnel. Specifically, the following conditions of use are established, which agents must observe to ensure the proper functioning of the systems:

- Download information that is not relevant for market operations (such as invoices) outside critical time windows (e.g., during the periods immediately prior to auction closing).
- Do not query information that is already available or that can be easily calculated by the agent. For example, schedules and invoices should be downloaded only once.
- In order to minimize redundant information volume and optimize the processing of communications performed by agents' applications, agents must send only those bid-modification actions that are strictly necessary, both in DAM and in IDAs, avoiding the submission of bid packages that include repeated orders whose information is already in the system and that show no variations.

- Refrain from submitting orders that are known in advance to end up being invalid because they exceed the unit's technical power ranges or the limits of available guarantees.
- Do not repeatedly access information whose status is known in advance not to have changed.
- Closely track errors reported by the system, avoiding resubmitting requests that have already been processed and have resulted in errors.
- The submission of auction bid files (both for DAM and IDAs) must be serialized, respecting the maximum number of orders per file (as described in Annexes I and II).
- Agents must notify in advance any downloads of large volumes of historical information through the support portal, providing as much detail as possible about the data they wish to request. Once the request is received, OMIE will inform the agents of the necessary conditions for carrying it out.

In addition to the points above, when access is via the WS API, agents must continuously monitor the performance of their applications and comply with the following guidelines:

- Do not make excessively frequent invocations of the services, even when the minimum times permitted by the system are respected.
- To download information in file format, invoke the published files service (*ServicioConsultaNuevosFicheros*) instead of attempting to directly and repeatedly download a file without knowing whether it has been published yet.
- Do not download via WS information that has already been previously obtained through CM LTS platform messages.

II. Terms of Use for CM access

Access to the Continuous Market may be via OMIE's Trading Client or via an application developed by the agent that also uses the Continuous Market API. In the latter case, the agent must have previously passed the Enablement process to operate in the production environment and must have internal control methodologies that ensure the proper functioning of their applications once connected to the CM trading platform.

Market agents are responsible for all CM access performed using the security certificates assigned to their company personnel. Specifically, the following conditions of use are established, which agents must observe to ensure the proper functioning of the systems:

- Agents must maintain an appropriate ratio between unexecuted orders and completed transactions (see Annex I), specifically avoiding the repeated

submission to the continuous market of orders whose likelihood of execution is null or unlikely.

- Do not submit orders that end up being invalid because they exceed the unit's technical power ranges or the limits of available guarantees.

In addition to the points above, when access is via an application developed by the agent that uses the Continuous Market API, agents must continuously monitor the performance of their applications and comply with the following guidelines:

- Refrain from using global (high-volume) information requests when such information has already been communicated to the application through the automatic incremental information dissemination mechanisms provided by the CM API.
- Closely track errors reported by the system, avoiding resubmitting requests that have already been processed and have resulted in errors.
- The application must be able to respond efficiently in high-trading situations by quickly consuming the messages made available by the CM trading platform in its private message queue.
- Do not make information requests that have already been previously obtained, or when the process can be executed more efficiently through the WS API.

C. Monitoring and enforcement of agents' obligations

OMIE will implement a series of applications, procedures, and mechanisms to ensure that agents' applications comply with the Terms of Use and cannot generate anomalies in trading conditions nor contribute to them. Control of agents' behavior will be performed both in real time and ex post through performance indicators of the activity carried out.

I. Real-time mechanisms

OMIE will apply real-time control mechanisms intended to keep agents' request rates within certain limits. The control mechanisms are described in detail in Annexes I and II, and are of three types:

- Limits on the number of orders that can be grouped in a single submission to the different markets.
- Minimum time thresholds between invocations of actions and/or information requests.
- Exclusion periods during which certain requests and/or actions may not be performed.



Agents who perform actions in breach of the above limits will receive an automatic response informing them of the event instead of the response to the requested action.

In order to ensure the continuous proper functioning of the market platforms, the control mechanisms, as well as the thresholds and parameters used, may be modified by OMIE according to system requirements.

OMIE also has real-time monitoring systems for access to its platforms, which provide detailed information on agents' activity (number of queries performed, breakdown by query type, total number of Web Services accesses, number of messages sent to the CM, AMQP performance, among others). If anomalies or abusive uses are detected from these monitoring, OMIE will adopt the reasonable and proportionate measures it deems appropriate.

II. Performance indicators

In order to protect the systems shared by all agents, OMIE establishes a set of performance indicators (KPIs) and associated limitations to monitor the proper use of the available access systems. The selected KPIs are described in detail in Annexes I and II. Their calculation and monitoring are performed periodically.

OMIE will monitor, through subsequent processes, that agents respect the established limits and will notify by email each time the limitation associated with any of the agents' performance indicators is exceeded. The agent must respond within a reasonable time frame, explaining the situation and the measures taken to prevent it from continuing, as well as providing any other additional information required by OMIE.

D. Actions in the event of non-compliance with agents' obligations.

If OMIE detects situations that put market operations at risk or abusive behavior, it will inform the agent through the contact persons registered on OMIE's Market Website. The agent must respond to the questions and instructions received and correct the reported behaviors within the established deadlines, including, if necessary, temporarily halting its access or disconnecting applications until the incident is fully resolved.

If it is the agent itself that detects a behavior of its application that does not follow the Terms of Use for access to the APIs or that violates limits of the control mechanisms or performance indicators, it will remedy the situation as soon as possible and will inform OMIE through the corresponding communication channels.



If the agent cannot be contacted through the contact person, or if the effects of the anomaly or abuse could cause short-term damage to the trading platforms, OMIE may take all reasonable and proportionate measures it deems appropriate to correct and/or mitigate the detected situation that puts the stability or performance of its platforms at risk. Among others, the following measures are contemplated:

- disconnecting the agent's application.
- preventing access by the agent's digital certificates responsible for the situation.
- preventing access by the agent responsible for the situation.
- preventing access by the applications responsible for the situation, including disabling third-party applications.

The measures above may also be applied if the agent disregards OMIE's instructions; fails to meet the deadlines set by OMIE to resolve reported incidents; fails to comply with a limitation tied to a certain performance indicator (beyond the number of times that indicator stipulates as a limit); or if OMIE detects that the agent's application is endangering the stability or performance of the platforms or market processes in any way.

3. APPLICATION

The content of this Instruction replaces that of Instruction 1/2022, and will apply from the time of its publication on OMIE's Public Website, with the exception of the obligation for applications developed by agents that use the Web Services API to pass a prior Enablement process before accessing production systems, as well as the provisions in the following sections of ANNEX I: "Minimum time between queries to the Market Website", "Exclusion periods for queries to the Market Website" and "Performance indicators for access to the Market Website" (PORAS), which will enter into force on the date that will be communicated later through OMIE's Market Website.

ANNEX I

CONTROL MECHANISMS AND PERFORMANCE INDICATORS

A. Real-time control mechanisms

I. Control of access to the Market Website

Minimum time between queries to the Market Website

Minimum times will be established between invocations of each query. It will not be possible to make a new invocation of the same query until that minimum time has elapsed since the last request.

- Per-certificate threshold: If a certificate exceeds the defined threshold for time between requests for a specific query, the platform will respond with a message informing of the breach instead of providing the requested information.
- Per-agent threshold: If two certificates belonging to the same agent submit requests to the same query in breach of the established threshold between invocations, the second certificate making the request will receive an informational breach message instead of the requested information.

Times will be counted from the moment the system receives the agent's query request.

If the agent does not respect the minimum intervals between requests, the new request, which will be rejected, will reset the counter. Therefore, the required minimum time will be counted again from the receipt of that failed request.

Annex II establishes the limits that will apply to each query.

Exclusion periods for queries to the Market Website

There will be certain exclusion periods during which, in order to streamline certain market processes (such as auctions), access to certain queries will be restricted. The objective is to avoid overloading these critical moments with requests that can be postponed. During such periods, the affected queries will not return information, and a message will be shown informing of this circumstance.

Annex II specifies which queries will have exclusion periods and what those periods will be.

Limits on the number of orders per file and restriction of simultaneous submissions

There will be a maximum number of orders allowed in each file sent to the Day-Ahead Market (DAM) or the Intraday Auction Market (IDA). This control, which will also apply to submissions made from the browser, will block the processing of files that exceed the established limits (Annex II). In such cases, the agent will receive an error message, and no bid will be processed.

In addition, once a bid file has been submitted, the agent may not submit a new file until it receives the response to the previous one. This control will apply per agent (not per certificate) and, if a second file is submitted while the response to the first is still pending, the system will return an error message and none of the orders in the second submission will be processed.

Real-time monitoring of access to the Market Website

OMIE will monitor a series of indicators that make it possible to detect those behaviors in access to the Market Website that are considered inappropriate and that are not aligned with those described in the Terms of Use. The following, among others, will be monitored:

- Breaches committed by agents by not respecting the established minimum times between submissions or the exclusion periods
- The number of queries per agent and certificate
- Accesses to each type of query
- Repeated requests with the same input parameters
- And any other indicator that OMIE deems necessary to monitor.

The situations described above will be monitored and, if they pose a real-time risk to market operations or may lead to behaviors that compromise such operations, they will be treated as a breach of the agent's obligations.

II. Control of access to the CM

Minimum time between invocations to the CM

There will be a restriction on the minimum time that must elapse between successive requests to the CM. The time limits will be defined by message type and will apply to requests made by each certificate. If the established time threshold is breached for a given message type, the system will notify the agent's application of this situation, informing of the event instead of providing the response to the request made.

Annex II describes the thresholds that will apply to each message type.

Maximum management action ratio (MRA) per unit of time in the CM

Límite máximo a la ratio de acciones de gestión sobre las ofertas (inserción, modificación, cancelación) que se pueden realizar por intervalo de tiempo. Las acciones que se verán limitadas, así como el intervalo mínimo de tiempo, están definidos en el Anexo II.

Real-time monitoring of CM access

OMIE will monitor a series of indicators that make it possible to detect those behaviors in access to the CM that are considered inappropriate and that are not aligned with those described in the Terms of Use. The following, among others, will be monitored:

- Breaches committed by agents by not respecting the established minimum times between submissions.
- The number of submissions made per agent and certificate in the last analyzed time period.
- Consumption of the messages from the broadcast queues that are associated with the application used by the agent.
- And any other indicator that OMIE deems necessary to monitor.

The situations described above will be monitored and, if they pose a real-time risk to market operations or may lead to behaviors that compromise such operations, they will be treated as a breach of the agent's obligations.

B. Performance indicators

I. Performance indicators for access to the Market Website

Percentage of Repeated Orders versus orders submitted per Agent and Session (PORAS)

Ratio, expressed as a percentage, between the number of orders that identically replace a bid previously submitted to a session and the total number of orders submitted by an agent to the auction platform for that same session (DAM or IDAs).

$$PORAS = \frac{\text{total number of repeated orders}}{\text{total number of orders sent}} \times 100$$

- PORAS will be calculated per session (DAM or IDAs) and per agent.

- A bid submitted by an agent for a session (DAM or IDAs) shall be understood as each of the orders registered in OMIE's system for that agent and session, and all subsequent versions thereof, regardless of whether they ultimately are valid or replaced.
- A bid shall be considered repeated in a session if it matches, across all its price/energy blocks for all periods, and across all variables corresponding to any complex conditions it may include, a bid from the same bidding unit, in the same direction (buy/sell) and with the same bid number (in the case of IDAs) that was previously submitted. If a repeated bid is submitted multiple times, each repetition shall count as a repeated bid.

A PORAS breach shall be deemed to have occurred when a bidding unit strictly exceeds the established threshold (UPORAS, whose value is set out in Annex II). If that limit is exceeded, the agent will be informed electronically of the event.

Within the same month, exceeding the UPORAS threshold will be allowed the number of times defined by parameter RPORAS (whose value is set out in Annex II). If this monthly limit is exceeded, the agent will be informed of the event and, in subsequent breaches, OMIE will apply the measures described in "Actions in the event of non-compliance with agents' obligations".

II. Performance indicators for CM access

Ratio of Orders versus Matched Orders per Bidding Unit and Contract (RUC)

Ratio between the total number of orders submitted by a bidding unit to the CM platform and the total number of orders that are matched (resulting in one or more *transactions*) per contract, in order to effectively ensure that such ratio does not lead to excessive volatility.

$$RUC = \frac{\text{total number of orders sent}}{\text{total number of orders matched}}$$

- RUC will be calculated on CM contracts once they have expired.
- Orders and transactions carried out by each bidding unit in each contract will be counted independently.
- Total number of orders: orders will be identified by the order identifiers assigned by the system. Modifying an order generally produces a new identifier.
- Total number of matched orders: these will be the orders executed partially or totally. When there are no matches, RUC will correspond to the orders submitted by the agent to the contract.

A RUC breach shall be deemed to have occurred when a bidding unit strictly exceeds the established threshold (URUC) in a contract (the value of URUC is set out in Annex II). If that limit is exceeded, the agent will be informed electronically of the event.

Within the same month, exceeding the URUC threshold will be allowed the number of times defined by parameter RRUC (whose value is set out in Annex II). If this limit is exceeded, the agent will be informed of the event. In subsequent breaches of this limit, OMIE will apply the measures described in “Actions in the event of non-compliance with agents’ obligations”.

Ratio of Orders versus Matched Orders per Agent and Traded Day (RAD)

Ratio between the total number of orders submitted by an agent to the CM platform and the total number of orders that are matched (resulting in one or more *transactions*) for all contracts of the same traded day, in order to effectively ensure that such ratio does not lead to excessive volatility.

$$RAD = \frac{\text{total number of order sent}}{\text{total number of orders matched}}$$

- RAD will be calculated on CM submissions across all contracts for a completed day.
- Total number of orders: these will be the orders submitted by the agent for the traded day. Orders will be identified by the order identifiers assigned by the system. Modifying an order generally produces a new identifier.
- Total number of matched orders: these will be the agent’s orders executed partially or totally on the traded day. When there are no matches for orders submitted in a contract belonging to the traded day, that contract will participate in RAD with the total number of orders submitted to it, and its contribution to the total number of matched orders (denominator) will be one unit.

A RAD breach shall be deemed to have occurred when an agent strictly exceeds the established threshold (URAD) for the traded day (the value of URAD is set out in Annex II). If that limit is exceeded, the agent will be informed electronically of the event.

Within the same month, exceeding the URAD threshold will be allowed the number of times defined by parameter RRAD (whose value is set out in Annex II). If this limit is exceeded, the agent will be informed of the event. In subsequent breaches of this limit, OMIE will apply the measures described in “Actions in the event of non-compliance with agents’ obligations”.

ANNEX II

Annex II can be consulted in the Monitoring and Access Control section of the OMIE Agents Documentation Website: <https://www.documentacion-agentes.omie.es/en/access-monitoring-and-control>