Information on conflicts of interest

Notice regarding authorisation status

Clovr Labs, S.L. has submitted to the Comisión Nacional del Mercado de Valores (CNMV) an application for authorisation as a crypto-asset service provider in accordance with Regulation (EU) 2023/1114 (MiCA).

As at the date of this publication, Clovr Labs, S.L. is not authorised as a crypto-asset service provider and does not provide crypto-asset services to clients.

The documents in this section describe the policies, terms and warnings that will apply from the commencement of the provision of the services, once authorisation has been obtained and registration in the relevant register has been effected. Their advance publication reflects a transparency criterion and does not constitute an offer, an invitation to contract or the marketing of crypto-asset services.

Clovr Labs, S.L.

Last updated: 22 July 2026

1. Purpose of this communication

Clovr Labs, S.L. ("**Clovr Labs**") has established policies, procedures and controls to identify, prevent and manage the conflicts of interest that may arise in the provision of crypto-asset services.

The purpose of this communication is to inform clients and prospective clients of:

- The situations that may give rise to conflicts of interest.
- The nature and source of those conflicts.
- The risks that could arise for clients.
- The measures adopted by Clovr Labs to prevent or mitigate them.

The publication of this information does not replace the organisational and control measures applied by Clovr Labs. This communication constitutes an additional transparency measure and is not regarded, in itself, as a sufficient means of managing a conflict of interest.

2. Crypto-asset services and the role of Clovr Labs

This communication relates to the crypto-asset services that Clovr Labs is authorised to provide and keeps available to its clients:

Custody and administration of crypto-assets on behalf of clients

Clovr Labs safekeeps or controls, on behalf of the client, crypto-assets or the means of access to them, including private cryptographic keys where applicable.

Execution of orders for crypto-assets on behalf of clients

Clovr Labs acts on behalf of the client in concluding agreements to purchase or to sell crypto-assets. In order to execute instructions, it may make use of liquidity providers, counterparties or other previously selected execution infrastructures.

Transfer of crypto-assets on behalf of clients

Clovr Labs executes, in accordance with the client's instructions, transfers of crypto-assets from one distributed ledger address or account to another.

Where several services are provided together, Clovr Labs will inform the client of the function and the capacity in which it acts at each stage of the transaction.

3. Persons and relationships that may give rise to conflicts

Conflicts of interest may arise between:

- Clovr Labs and its clients.
- Two or more clients with opposing interests.
- Clovr Labs and its shareholders or members.
- Clovr Labs and persons linked to it directly or indirectly by a control relationship.
- Clovr Labs and the members of its management body or its employees.
- Clovr Labs and its consultants, advisers, liquidity providers, technology providers, outsourced entities, subcontractors or other providers.
- Different areas or lines of business of Clovr Labs.

They may also arise where a director, employee, shareholder or other linked person holds economic interests or maintains personal, professional or political relationships capable of affecting their objectivity and independence.

4. Principal conflicts of interest and measures adopted

4.1. Interests of shareholders, directors, employees and linked persons

Source and nature of the conflict

Shareholders, directors, employees or other linked persons may hold shareholdings, crypto-assets, debt instruments, contractual arrangements, external professional activities or personal, professional or political relationships with clients, issuers, providers, counterparties or competitors of Clovr Labs.

Those circumstances could influence, or give the appearance of influencing, the objectivity with which decisions relating to a client or a service are taken.

Risks to the client

The principal risk is that a decision may be taken having regard to the particular interest of the linked person, of Clovr Labs or of a third party, rather than to the legitimate interest of the client.

Mitigation measures

Clovr Labs applies, among others, the following measures:

- Declaration and updating of interests and external activities.
- Assessment of such situations by the Compliance Function.

- Obligation to abstain from decisions affected by a conflict.
- Reassignment of functions or decisions to persons who are not affected.
- Controls over personal transactions in crypto-assets.
- Restricted lists and a requirement for prior authorisation where necessary.
- Documentation of the conflict and of the decision taken.
- Escalation of material conflicts to the management body.

4.2. Remuneration, commercial targets and fees

Source and nature of the conflict

Clovr Labs may receive commissions, fees or margins for the services provided. Likewise, certain employees or collaborators could be subject to targets or variable remuneration components.

Those circumstances could create an incentive to increase transaction volumes, assets held in custody, transfers, fees or margins, even where this is not in the client's interest.

Risks to the client

There could be a risk that a transaction or a form of service is recommended, prioritised or executed on account of its greater profitability for Clovr Labs or for the person involved.

Mitigation measures

- Remuneration is not determined exclusively by volume or by the revenue generated.
- Criteria relating to service quality, conduct, regulatory compliance and client protection are incorporated.
- Compliance reviews in advance the indicators and incentive systems capable of affecting crypto-asset services.
- Direct remuneration links between incompatible activities are removed where they may give rise to a conflict.
- Third-party inducements that would compromise the honest, fair and professional conduct of Clovr Labs are not permitted.
- Conflicts arising from remuneration or incentives are recorded in the conflicts register.

4.3. Selection of providers, counterparties and liquidity providers

Source and nature of the conflict

Clovr Labs may use technology providers, identity verification platforms, infrastructure providers, liquidity providers or other counterparties.

A conflict could arise if Clovr Labs or a linked person were to maintain an economic, contractual or personal relationship with one of those third parties, or if Clovr Labs were to receive discounts, commissions, advantages or benefits connected with their selection.

Risks to the client

The third party could be selected having regard to links or advantages for Clovr Labs rather than to criteria of security, quality, price, solvency or outcome for the client.

Mitigation measures

- Objective selection and due diligence procedures.
- Assessment of the third party's capacity, security, solvency and quality.
- Declaration of linked relationships.
- Prior review by Compliance where a potential conflict exists.
- Contractual obligations of confidentiality, cooperation and notification of conflicts.
- Periodic monitoring of the provider's quality and performance.
- Analysis of alternatives where reasonable.
- Prohibition on accepting inducements liable to harm the client.

4.4. Conflicts between clients

Source and nature of the conflict

Two or more clients may have opposing interests, in particular as regards the priority of orders or transfers, the allocation of operational resources, the handling of incidents or access to information.

Risks to the client

Clovr Labs could favour, or give the appearance of favouring, certain clients on account of their volume, connection, profitability or commercial relationship.

Mitigation measures

- Objective and non-discriminatory rules on priority and treatment.
- Observance of the chronological order of instructions where applicable.
- Separation and confidentiality of each client's information.
- Prohibition on promoting transactions that benefit one client to the detriment of another.

- Recording and review of exceptions.
- Oversight by the Operations and Compliance functions.
- Review of complaints and incidents capable of revealing unequal treatment.

4.5. Access to and use of confidential information

Source and nature of the conflict

Authorised personnel may have access to information on balances, wallets, transactions, pending transfers, orders, incidents, providers or internal decisions.

Risks to the client

The information could be misused in order to carry out personal transactions, to benefit another client or a third party, to anticipate an order or to take commercial decisions contrary to the client's interest.

Mitigation measures

- Access limited in accordance with each person's functions and with the need-to-know principle.
- Access controls and activity logs.
- Information barriers between incompatible functions.
- Duties of confidentiality.
- Controls over personal transactions and restricted lists.
- Specific training and disciplinary measures.
- Investigation of unauthorised access or use.

4.6. Unregulated technology activity

Source and nature of the conflict

In addition to its crypto-asset services, Clovr Labs develops software and provides technology services to third parties. A client or provider of that activity could coincide with a client, provider, counterparty or commercial partner of the regulated activity.

A conflict could also exist in the allocation of personnel, resources or information between the two lines of business.

Risks to the client

The technology activity could receive preferential treatment, obtain access to client information or influence decisions relating to the crypto-asset services.

Mitigation measures

- Distinct identification of functions and responsibilities.

- Documentation of the time devoted by the persons taking part in both activities.
- Restriction of access to information.
- Segregation of functions where necessary.
- Specific review by Compliance of overlapping relationships.
- Recording and monitoring of the conflicts identified.

5. Service-specific conflicts

5.1. Custody and administration of crypto-assets

In custody, conflicts may arise in relation to:

- The use, mobilisation or encumbrance of clients' crypto-assets for the benefit of Clovr Labs or of third parties.
- The commingling of own assets and clients' assets.
- The selection of infrastructures, wallet, security or technology service providers.
- The treatment of forks, airdrops, migrations, economic rights or participation rights.
- The priority of withdrawals or returns during incidents, maintenance or congestion situations.
- The attribution of liability for losses, errors or security incidents.
- Access to information on clients' positions and movements.

In order to mitigate those risks, Clovr Labs applies the prohibition on using clients' assets for its own account, operational and accounting segregation, reconciliations, enhanced controls over keys and wallets, objective criteria for the treatment of events and withdrawals, documented investigation of incidents and oversight by Compliance.

5.2. Execution of orders

In the execution of orders, conflicts may arise in relation to:

- The selection of liquidity providers, counterparties or execution mechanisms.
- The existence of economic or contractual relationships with those providers.
- The application of spreads, margins, fees or costs.
- The priority, sequencing, aggregation or allocation of orders.

- The use of information on pending orders.
- The handling of errors, delays or execution failures.
- Remuneration linked to the volume executed or to the use of a particular provider.

Clovr Labs applies objective criteria for the selection and review of providers, execution quality controls, transparency of prices and costs, traceability of orders, priority rules, controls over confidential information, error correction procedures and a prohibition on inducements liable to compromise the proper execution of the client's instructions.

5.3. Transfer of crypto-assets

In transfers, conflicts may arise in relation to:

- The priority of processing during congestion or high-demand situations.
- The selection of routes, networks, infrastructure providers or fee levels.
- The application of surcharges or network fees.
- The blocking, delay or rejection of a transfer on grounds of security, fraud, sanctions, anti-money laundering, the Travel Rule or operational risk.
- The handling of address errors, incorrect networks, duplications or failed transfers.
- The provision of the transfer service in combination with custody or execution.

Clovr Labs applies objective processing criteria, chronological traceability of instructions, transparent information on charges, non-discriminatory security and compliance controls, review of false positives, procedures for handling errors and separation of the decisions relating to the different services.

6. Governance and oversight

The Compliance Function is responsible for coordinating the identification, assessment, recording and monitoring of conflicts of interest. It has independence, authority, access to information and direct communication with the management body.

The management body is responsible for approving, implementing and reviewing the Conflicts of Interest Policy and for ensuring that the deficiencies identified are remedied.

Clovr Labs maintains an up-to-date register of actual and potential conflicts, the persons and services affected, the assessment carried out, the measures adopted, the final decision and whether the conflict was disclosed to the client. The records are retained for a minimum period of five years.

The effectiveness of the policy and of its controls is reviewed periodically and, as a minimum, once a year, as well as where new services or products are introduced, organisational or regulatory changes occur or material incidents or complaints are identified.

7. Specific disclosure of conflicts

Where Clovr Labs identifies that the organisational and administrative measures applied do not make it possible to prevent, with reasonable certainty, the risk of damage to a client, it will provide the client, before providing the service concerned, with specific information on:

- The nature, source and circumstances of the conflict.
- The service in relation to which it arises.
- The specific risks to the client.
- The measures adopted to mitigate it and their limitations.

The information will be provided in sufficient detail to enable the client to take an informed decision as to whether to use, or to continue to use, the service.

Where a conflict cannot be adequately prevented or managed, Clovr Labs may refrain from commencing or continuing the service or transaction concerned.

8. Enquiries and notification of possible conflicts

Clients and prospective clients wishing to obtain further information or to report a situation liable to give rise to a conflict of interest may use the customer service and contact channels made available by Clovr Labs on this website.