Summary of the Crypto-Asset Transfer Policy

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.

Web version 1.0 — Last updated: 6 August 2026

1. Introduction and regulatory status

Clovr Labs, S.L. ("Clovr" or the "Entity") has applied to the Comisión Nacional del Mercado de Valores ("CNMV") for authorisation as a crypto-asset service provider in accordance with Regulation (EU) 2023/1114 ("MiCA"). The service described will only be provided once authorisation has been granted and is effective, and within the authorised scope. The publication of this summary does not mean that authorisation has already been granted.

This summary contains the main information on the conditions, procedures and rights associated with the transfer service. It will be construed together with the service agreement, the pre-contractual information, the full policy and the security, risk, anti-money-laundering and customer-service policies. Before contracting, the Client will receive this information in electronic format and will be able to access it or request it throughout the contractual relationship.

Provider details and regulatory status

Company name: Clovr Labs, S.L.

Tax ID (NIF): B67306894.

Registered office: Avenida de la Generalitat, 24, 08840 Viladecans, Barcelona, Spain.

Postal and contact address: Carrer Santa Eulàlia, 5, 3rd floor, 08012 Barcelona, Spain.

Email: hello@clovrlabs.com.

Website: www.clovrlabs.com.

Competent authority: Comisión Nacional del Mercado de Valores (CNMV), before which the application for authorisation is being processed and which will supervise Clovr once authorised.

Chapter I. Features of the service

Article 1. Purpose and scope

The service will allow the Client to instruct the total or partial sending of crypto-assets held under Clovr's custody or administration to another crypto-asset account or distributed-ledger-technology (DLT) address. The service will initially be aimed at legal-person Clients incorporated in Member States of the European Union. The only supported crypto-asset will be Bitcoin (BTC) and the only admitted network will be the Bitcoin network. Any extension will be communicated before it is applied.

As a general rule, Clovr will only accept transfers whose beneficiary is the Client itself or whose destination can reasonably be attributed to the Client. Transfers to third parties, to self-hosted addresses or to non-validated providers will only be processed where Clovr expressly permits them and after completing the applicable enhanced controls. The Policy will also apply to transfers required by a legal obligation or by a judicial or administrative order.

Article 2. Channels, communications and technical requirements

Instructions and communications will be processed through the Client's private area, electronic notifications and other previously validated secure channels. The Client must have an internet connection, a compatible browser or software, access to the required authentication mechanisms and up-to-date contact details. The agreement and communications will be provided in Spanish or English, according to the language of contracting.

The information will be provided in electronic format. The confirmation of each transaction will be made available without undue delay, and the standard periodic information will be provided, as a minimum, monthly and free of charge where it is not provided more frequently.

Chapter II. Initiation, consent and execution

Article 3. Initiation of the order and required information

The order must identify, as a minimum, the originator and the beneficiary, the crypto-asset, the amount, the DLT network, the origin and destination address or account and, where appropriate, the beneficiary's service provider. Clovr may request evidence of ownership or control of the address, information on the economic purpose and any additional documentation necessary to comply with the rules or to manage risk.

An incomplete, contradictory or insufficient order will not be considered ready for execution until the Client provides the required information.

Article 4. Prior information, consent and withdrawal

Before the Client confirms each transfer, Clovr will display a summary including the asset, amount, network, destination, maximum execution time and all foreseeable expenses, charges and fees, breaking down the DLT network charges and Clovr's fees where appropriate. The specific amount will be shown before confirmation and will be construed together with the pricing, costs and fees policy published by the Entity.

The summary will include a clear warning that an incorrect address or network, and the broadcasting of the transaction, may cause an irreversible loss. The order will be deemed consented to and received when the Client confirms it by means of the required authentication mechanism.

Complete orders confirmed on a business day before 17:00, mainland Spanish time, will be deemed received on that day; those confirmed after that time or on a non-business day will be deemed received on the following business day. The Client may withdraw the order up until the moment immediately before it is broadcast to the Bitcoin network. After broadcasting it will, as a general rule, be irrevocable.

Article 5. Prior checks and Travel Rule

Before executing a transfer, Clovr will verify the identity and powers of the originator, the available balance, the compatibility between BTC, the Bitcoin network and the destination, the formal correctness of the address and the consistency of the transaction. It will also apply the obligations of Regulation (EU) 2023/1113 on information accompanying transfers, the measures for the prevention of money laundering and terrorist financing, sanctions screening and fraud and security controls.

Where the information on the originator, the beneficiary or the transfer is missing, incomplete, inconsistent or insufficient, Clovr may request additional information, suspend, reject or return the transaction. It may apply enhanced measures or restrictions in respect of providers that repeatedly fail to comply with their information obligations.

For transfers to or from a self-hosted address in an amount equal to or greater than EUR 1,000, calculated upon receiving or validating the order and excluding fees, Clovr will verify the ownership or control of the address by means of a cryptographic signature, a micro-transfer, remote or in-person verification, sufficient technical evidence or another method appropriate to the risk.

Article 6. Execution time and irreversibility

Once the checks have been completed, Clovr will execute the transfer without undue delay and within the communicated time. Unless the agreement establishes a different time limit for a particular case, the maximum operational time limit will be seven calendar days from the receipt of a complete and firm order. The count may be suspended while essential information is missing or where an incident temporarily prevents execution.

On the Bitcoin network, Clovr will generally consider that the transfer has reached a sufficient degree of irreversibility after three block confirmations. Depending on the amount, the risk or the network circumstances, a higher number may be required.

Article 7. Rejection, suspension or return

Clovr may reject, suspend or return a transfer where the information is incorrect, false, out of date or incomplete; there is an incompatibility of asset, network or destination; the required ownership or legitimacy cannot be verified; there are indications of fraud, money laundering, terrorist financing or breach of sanctions; or legal, contractual, technical or security limitations apply.

Clovr will inform the Client without undue delay, provided that the law and the purpose of the controls so permit, of the reason, of the way to remedy the incident and of the charges incurred, indicating whether they are to be refunded. If a period for remedying the situation is granted and it elapses without a sufficient response, the order may be cancelled.

Chapter III. Client information and security

Article 8. Post-transaction information

Following execution, Clovr will provide the Client, in electronic format, with a confirmation that makes it possible to identify and verify the transaction. It will include, as a minimum, the names of the originator and the beneficiary, the origin and destination accounts or addresses, a transfer reference, the type and amount of crypto-asset, the corresponding date and time or value date, the charges applied and their breakdown and, where one exists, the hash or technical identifier of the transaction.

If the transfer is rejected, returned or suspended, the communication will state its status, the main cause, the possible corrective measures and the information on the charges and their possible refund.

Article 9. Fraud, security threats and Client duties

Where there are indications of fraud, deception, credential takeover or a relevant threat, Clovr may contact the Client through validated channels, request additional confirmations, temporarily delay execution or prevent it while it completes its analysis. Clovr's security notifications will be made through the secure channels communicated to the Client.

The Client must safekeep its credentials and authentication mechanisms, maintain control of its devices and report without delay any loss, compromise or unauthorised use that may affect the service.

Article 10. Unauthorised or incorrectly executed transfers

The Client must notify any transfer that it considers unauthorised or incorrectly initiated or executed without undue delay and, in any event, within the thirty calendar days following becoming aware of the incident, using the private area, the customer-service department or the other secure channels made available. Clovr will acknowledge receipt, investigate the consent, the execution and the origin of the incident and communicate the outcome.

Clovr will be liable to the Client for transfers executed without valid consent or incorrectly executed for reasons directly attributable to the Entity, and will adopt the reasonable measures of restitution or compensation provided for in the agreement and in the applicable rules. The agreement will specify, before contracting, the scope and the maximum amount of that liability. Clovr will not be liable for losses arising from erroneous information provided by the Client, an incompatible network or destination, fraudulent or grossly negligent conduct by the Client, the ordinary operation of the network after broadcasting, measures taken by authorities or circumstances beyond its reasonable control, unless mandatory rules provide otherwise.

Chapter IV. Access, changes and termination

Article 11. Access to documentation and amendments

Throughout the contractual relationship, the Client may access or request, in electronic format, a copy of the transfer agreement, of this information and of the applicable version of the Policy. Clovr will communicate any relevant change with sufficient advance notice and, where appropriate, at least one month before it takes effect. The Policy will be reviewed at least annually and whenever there are relevant regulatory, operational or technological changes.

Article 12. Termination, applicable law and records

The Client may terminate the contractual relationship on the terms of the agreement, without prejudice to the orderly settlement of pending transactions. The applicable law and the dispute-resolution mechanisms will be those established in the agreement, without prejudice to the mandatory rules of MiCA and of Spanish law.

Clovr will retain complete and traceable records of orders, checks, decisions and communications for the legally required period and, as a minimum, five years from the transaction, or ten years where required by anti-money-laundering rules. Personal data will be processed in accordance with data-protection rules and for purposes connected with the service, legal compliance and risk management.