Summary of the Custody 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 Labs" 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 custody 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 Clovr Labs is already authorised.

This document summarises the principles and controls of Clovr Labs's Custody Policy. It will be made available in electronic format to Clients who request it and will remain available on the website. The full Policy, the service agreement and the pre-contractual documentation will prevail in the event of any discrepancy.

2. Purpose and scope

The Policy governs the custody and administration of crypto-assets on behalf of Clients and the safekeeping of the means of access, in particular private cryptographic keys. The service will initially be aimed at legal-person Clients admitted in accordance with Clovr Labs's onboarding policy, and the only supported crypto-asset will be Bitcoin (BTC).

In order to provide the service, Clovr Labs will enter into an agreement with each Client that will identify the parties, describe the service and the custody policy or summary, and govern the means of communication and authentication, the security systems, the fees and expenses and the applicable law. The Client will be allocated an individualised record of positions and transactions.

3. Essential custody principles

- identify and distinguish at all times the crypto-assets belonging to each Client from those of other Clients and from those of Clovr Labs itself;
- keep records that make it possible to reconcile internal positions with the addresses and balances existing on the DLT;
- minimise the risk of loss, deterioration, fraud, cyberattack, error, misuse or negligence;
- not use Clients' crypto-assets for its own account;
- not block or restrict access unless there is a duly justified legal, contractual, security or risk-management ground;
- document the relevant instructions, transactions, reconciliations, incidents and communications; and
- return the crypto-assets to the Client as soon as possible following a valid request or the termination of the service.

4. Segregation, records and reconciliation

Clovr Labs will maintain a segregation system at the level of accounts, zones, wallets and DLT addresses. The addresses in which Clients' crypto-assets are recorded will be kept separate from those used for own positions, and Clovr Labs will not add own positions to Clients' omnibus accounts.

Clovr Labs may use global or omnibus addresses in which the crypto-assets of several Clients are recorded, always on behalf of third parties. In such cases, the internal records will make it possible to identify the individual position of each Client at all times, including for insolvency purposes, and to reconcile it with the positions on the Bitcoin network.

DLT accounts and positions will be reconciled daily. Any discrepancy will be investigated, documented and resolved in accordance with the applicable internal procedure. Records will be retained in a complete, traceable and audit-ready manner for the legally required period.

5. Key custody and security measures

Custody comprises the generation, storage, safekeeping and control of private keys and, where applicable, of backup material. Clovr Labs will retain operational control of the keys in its custody and will not give the Client access to them, unless the service uses a 2-of-3 multi-signature scheme with Client co-signing. In that case, the Client may retain one of the keys, without any capacity for unilateral disposal, and will be responsible for safekeeping it diligently.

Keys will be generated and used by means of certified hardware security modules or equivalent controls, will be configured as non-exportable where appropriate, and will be subject to encryption, segregation of duties, dual access, least privilege and audit logs. Backups will be kept protected, fragmented and segregated in accordance with the internal procedures.

Clovr Labs's wallets will operate under a 2-of-3 multi-signature scheme. Warm wallets, connected to the internet for day-to-day activity, will hold only the minimum necessary balances and will be subject to limits and authorisations. The majority of crypto-assets will be kept in offline cold wallets, with manual procedures and enhanced access controls. Clovr Labs will apply a documented life cycle for the generation, activation, use, rotation, revocation, recovery and invalidation of keys.

6. Risk and incident management

Clovr Labs will identify, assess and periodically review the operational and information-technology risks associated with custody, including the loss or compromise of keys, unauthorised access, fraud, cyberthreats, human error, infrastructure or provider failures, network unavailability and reconciliation errors. It will apply technical, organisational and documentary measures proportionate to the risk.

If a loss of crypto-assets or of means of access occurs, Clovr Labs will inform the Client without undue delay of the incident and of the measures adopted to mitigate its impact, unless a legal prohibition prevents certain information from being provided.

7. Information and position statements

Clovr Labs will provide each Client, at least once every three months and whenever the Client so requests, with a position statement in electronic format identifying the crypto-assets recorded in the Client's name, the balance, the value in accordance with the applicable methodology or source, and the transfers carried out during the period. It will also communicate as soon as possible any transaction or event that requires a response from the Client.

8. Return of crypto-assets

Clovr Labs will return the crypto-assets or the means of access to their holder as soon as possible following a valid request or the termination of the service. Before returning them it will verify the identity and powers of the requester, ownership and balance, the destination address and the controls relating to the prevention of money laundering, sanctions, fraud and security, and it will retain evidence of the instruction and of the transaction.

Clovr Labs will not impose, as the sole option, the return of the value in fiat money or of another equivalent crypto-asset in substitution for the crypto-assets held in custody, unless the Client voluntarily and additionally accepts this and the applicable rules permit it.

9. Associated rights and network events

Where appropriate, Clovr Labs will facilitate the exercise of the rights associated with the crypto-assets held in custody and will record without delay the events that may create or modify the Client's rights. Forks, airdrops, migrations, redenominations, token swaps and protocol changes will be assessed and communicated where they may affect those rights, in accordance with the terms and exclusions set out in the agreement and in the applicable rules.

10. Sub-custody and outsourcing

Clovr Labs will not delegate the custody, administration or control of crypto-assets or means of access without a prior assessment, internal approval, information to the Client and compliance with the regulatory requirements. The third party must be authorised or entitled where required, and the arrangement will govern, among other matters, its functions, any sub-delegations, conflicts of interest, service levels, audit rights, ongoing oversight, continuity and exit plan. Outsourcing will not reduce Clovr Labs's liability towards the Client.

11. Liability

Clovr Labs will be liable to the Client for the loss of crypto-assets or of the means of access where this results from an incident attributable to the Entity. If the loss is attributable to Clovr Labs, its liability will be limited to the market value of the affected crypto-assets at the time the incident occurred, without prejudice to any applicable mandatory rules.

A loss caused by circumstances beyond its control, or where it is shown that the event would have occurred regardless of the custody service, will not be regarded as attributable to Clovr Labs. Custody likewise does not eliminate market risk nor guarantee the value of BTC.

12. Governance, review and access

The management body will approve and oversee the Policy and will allocate sufficient resources for its implementation. A Crypto-Asset Custody Officer will coordinate the protection of the assets and means of access, develop the procedures and report periodically to senior management.

The Policy and its procedures will be reviewed periodically and whenever there are relevant regulatory, operational, technological or risk-related changes. The Client may at any time request an updated electronic copy of this summary and consult the version published at www.clovrlabs.com.