Summary of Custody Policy

MP Developers s.r.o.

Version as of 1 July 2026

1 Introduction and Purpose of the Document

In this document, MP Developers s.r.o. (hereinafter referred to as the "**Provider**") summarises the basic principles for handling funds and crypto-assets entrusted to the Provider by the Client, or otherwise held or controlled by the Provider in connection with the provision of Services to Clients, including their custody and administration, in accordance with Articles 70(1) to (3) and 75(1) and (3) of the Regulation.

The terms used in this Summary of Custody Policy have the meaning defined in the Anycoin Platform Terms and Conditions (hereinafter referred to as the "**Anycoin Platform Terms and Conditions**") and the Platform Services Agreement (hereinafter referred to as the "**Platform Services Agreement**").

In the event of any conflict between this Summary of Custody Policy and the Terms and Conditions or the Platform Services Agreement, the Terms and Conditions and the Platform Services Agreement shall prevail.

All information provided in this manner will remain valid for the duration of the Platform Services Agreement, or during the period of validity of the relevant version of the Summary of Custody Policy, should this document be amended during the term of the Platform Services Agreement.

2 Measures to ensure the separation of Clients' crypto-assets and funds, and to protect their ownership rights

The Provider stores, records and manages the Client's crypto-assets and funds separately from the Provider's own crypto-assets and funds, ensuring the protection of the Client's ownership rights and preventing the use of crypto-assets and funds for its own account through a combination of the following measures:

Separate Wallets

The Provider uses a different set of Wallets for the Custody and Administration of its own crypto-assets and for those of its Clients. The Provider also applies a strict hierarchy of Wallets for the Custody and Administration of Clients' crypto-assets.

Separate bank accounts

The Provider uses operational accounts to record its own funds, and maintains a separate bank account for collecting and recording the Client's funds. This separate bank account is maintained under a special regime, as set out in Section 41f of Act No. 21/1992 Coll., on Banks.

Separate records at Partner Exchanges

Within the framework of Partner Exchanges, the Provider creates and maintains two types of user profiles and the associated records within bank accounts and the Partner Exchange's internal records – the Provider's account as a provider of crypto-asset-related services in accordance with the Regulation, when acting on behalf of Clients, and the Provider's own account, when acting on its own behalf.

Access rights policy in relation to Wallets

The Provider applies a policy for access and signature rights and processes, which is established separately for Wallets used for the Custody and Administration of the Provider's crypto-assets and for Wallets used for the Custody and Administration of Clients' crypto-assets.

Policy of disposal authorisations in relation to bank accounts

The Provider applies a policy of disposal rights in relation to a separate bank account.

Accounting separation

The Provider's accounting system ensures that crypto-assets and funds owned by the Provider are kept separate from those owned by Clients, and that related transactions, balances and receivables are recorded separately.

Legal separation

Based on the Terms and Conditions, crypto-assets and funds belonging to Clients are considered third-party assets in relation to the Provider, and therefore, under the legal order of the Czech Republic, which is the governing law, such assets do not become part of the Provider's assets in the event of the Provider's insolvency (bankruptcy).

Records separation

The Provider achieves records separation between its own crypto-assets and funds and those of its Clients, as well as between the crypto-assets and funds of one Client and those of another Client, by maintaining internal records that are subject to regular data reconciliation.

Organisational structure

The Provider has established the competences and authorities of its organisational units and employees in the provision of Services in such a way as to minimise the risk of using Clients' crypto-assets or funds for the Provider's own account.

Internal control and audit

The Provider implements internal controls over the handling of Clients' assets, including regular internal and external audits and verification of the adequacy of measures taken to separate and protect Clients' crypto-assets and funds.

3 Management and storage of funds

3.1 Separate bank account

The Provider holds Clients' funds entrusted in connection with the provision of Services in a separate bank account maintained by a bank based in the Czech Republic. This bank account is held under a special regime, as set out in Section 41f of Act No. 21/1992 Coll. on Banks, and is therefore distinguishable from any operational accounts used for the Provider's own funds.

If the Client has entrusted the Provider with funds in a manner other than by transferring them to the Provider's separate bank account (e.g. via a payment gateway), as set out in the Terms and Conditions, the Provider shall ensure that the entrusted funds are placed in the Provider's separate bank account by the end of the next business day.

When selecting a bank to hold a special regime account on behalf of the Provider, the Provider considers a number of criteria that are in the best interests of Clients, such as the bank's reputation, including an absence of negative publicity, its overall exposure, and its stable outlook for maintaining the Provider's account.

3.2 Funds to maintain liquidity on Partner Exchanges

For the purpose of ensuring sufficient liquidity for the timely provision of the Services, specifically the Execution of Orders Service, the Provider maintains the necessary amount of Clients' funds in the form of advances for Order execution in the Partner Exchanges' bank accounts. The Provider ensures the Transfer of Client funds to the bank accounts of Partner Exchanges through a payment service provider. Based on agreements with Partner Exchanges, the Client funds recorded in these bank accounts are kept separate from the Provider's funds. The internal records kept by the Provider relating to the Partner Exchange accounts are also used to separate one Client's funds from those of other Clients, as well as from the Provider's own funds. Partner

Exchanges are subject to the Regulation and other related legal requirements to a similar extent as the Provider, ensuring a comparable standard of protection for Clients' funds.

4 Management and storage of crypto-assets

4.1 Basic principles of storing crypto-assets

For the registration, custody and administration of Clients' crypto assets, the Provider uses several types of address or wallet to store them.

The Provider uses the omnibus wallets to store Clients' crypto-assets, meaning the crypto-assets of multiple Clients are stored together in a single wallet. The Provider ensures the separation of individual Clients' crypto-assets by maintaining internal records relating to individual wallets to ensure the continuous and unambiguous identification of the crypto-assets belonging to a specific Client.

As part of the Services provided, the Provider does not hold Clients' means of accessing their crypto-assets (i.e. their keys). The system for storing Clients' crypto-assets is based on the principle of collective registration of these assets in individual wallets, which are controlled by keys held by the Provider.

4.2 Wallet hierarchy

The Provider uses a multi-level hierarchy of wallets to ensure the protection and liquidity of the Clients' stored crypto-assets. Specifically, these are:

(a) **Wallets (accounts) of Partner Exchanges**, which the Provider uses to store Clients' crypto-assets in the minimum volume necessary to execute Clients' Orders. Partner Exchanges, when providing the Custody and Administration Services, are subject to the Regulation and other related legal requirements to a similar extent as the Provider, ensuring a comparable standard of protection for Clients' crypto-assets.

(b) **Hot wallets** are online wallets used for operational purposes, including the withdrawal and deposit of crypto-assets. The volume of crypto-assets held in these wallets is limited by the liquidity management policy.

(c) **Cold wallets (medium-term)** are offline wallets used by the Provider for the medium-term storage of crypto-assets. The volume of crypto-assets held in these wallets is limited by the liquidity management policy.

(d) **Cold wallets (long-term)** are offline wallets used by the Provider for the long-term storage of crypto-assets. This type of wallet holds the maximum possible volume of crypto-assets, which, in accordance with the liquidity management policy, are not stored in other categories of wallets.

4.3 Use of Partner Exchanges within the Custody and Administration Service

In accordance with the applicable legal regulations, the Provider uses part of the Client's crypto-assets stored at the addresses (wallets) of Partner Exchanges authorised to provide custody and administration of crypto-assets on behalf of the Client, for the proper and timely provision of the Execution of Orders Service.

When selecting Partner Exchanges, the Provider applies a due diligence process to ensure that the standard of protection of Clients' crypto-assets meets the requirements of the Regulation. The Provider reviews the fulfilment of these factors annually. The range of Partner Exchanges is defined in the table below.

Trade name of Partner Exchange	Operator of Partner Exchange	State authorisation under the Regulation

Kraken	Payward Europe Solutions Limited	IE

The Provider does not use another provider of services related to crypto-assets for the custody and administration of the Client's crypto-assets, except for the use of addresses (wallets) of Partner Exchanges in accordance with this article of the Summary of Custody Policy.

5 Record of Clients' funds and crypto-assets, and measures to facilitate the exercise of Clients' rights

Through its internal record-keeping system, the Provider ensures the continuous and unambiguous identification of each Client's crypto-assets and funds in a manner that enables them to be distinguished from those of other Clients and from the Provider's own funds and crypto-assets at any time. Internal records also include wallets or accounts of Partner Exchanges where the crypto-assets and funds of each Client are recorded. These records also serve as a register of positions as defined in the Regulation.

The Provider displays the status of internal records relating to the Client in their Client Account, and generates a statement from these records once every 3 months, which also serves as a declaration of the position of the crypto assets as defined in the Regulation.

If a response from the Client is required in relation to the registered crypto-assets (for example, if voting rights need to be exercised in the case of custody of governance tokens, or in the event of a hard fork of the DLT in use), the Provider will make this information available to the Client via their Client Account and, at the same time, ensure an appropriate response in accordance with the Terms and Conditions.

If an event occurs that is likely to affect the Client's rights in relation to the relevant crypto-asset (for example, a change in the DLT used = a fork, the right to claim an airdrop, or the accrual of staking rewards), the Provider will inform the Client and, at the same time, ensure an appropriate response.

The Provider's internal records are subject to regular daily reconciliation.

6 Procedures and deadlines for the return of crypto-assets

The Provider allows the return or payout of registered crypto-assets to the Client in the following three ways:

a) **Exchange** or **Execution of Order** for sale of crypto-assets, followed by payment of funds to the Client.

b) **Transfer to a third party** based on a Transfer Order submitted by the Client, and

c) **Direct Transfer** (withdrawal of crypto-assets) based on an Order **to an external Wallet, i.e. the Client's address**, either hosted or self-hosted, that is technically compatible with the Platform, including a wallet from another provider of services related to crypto-assets.

As part of the Services provided, the Provider does not hold Clients' means of accessing their crypto-assets (i.e. their keys).

The deadlines for the return or payout of crypto-assets depend on the volume of crypto-assets and the related technical capabilities of the wallet hierarchy. For crypto-assets not exceeding the equivalent value of EUR 10,000, the Provider will usually process the payment within 48 hours. For amounts exceeding this value, the Provider will inform the Client of the relevant deadline on a case-by-case basis.

7 Provider's liability for loss of crypto-assets

The Provider shall be liable to the Client for loss of crypto-assets resulting from an incident attributable to the Provider, up to the market value of the lost crypto-assets at the time of loss.

Incidents that cannot be attributed to the Provider include any event that occurred independently of the provision of Custody and Administration Services or the Provider's transactions, such as an issue with the functioning of the DLT, which is not controlled by the Provider. Further details are set out in the Terms and Conditions.

8 Operational and ICT risk management within the Custody and Administration of Client assets

As part of the custody and administration of Clients' assets, the Provider manages related operational risks, including those in the ICT area. Detailed procedures shall be determined by the internal regulations of the Provider.

Operational risks

Operational risks may arise from inadequate or failing internal processes of the Provider, human errors, system failures, or external events. The main sources of operational risks are:

- **Human error**: Errors made by the Provider's staff in key management, transaction execution or internal record maintenance.
- **Process failures**: Weaknesses in internal procedures for transaction approval, record maintenance or reconciliation processes.
- **Physical security**: Risks associated with physical access to critical infrastructure, such as servers or hardware security modules (HSM).

ICT risks

ICT risks include vulnerabilities in the infrastructure used for the Custody and Administration of crypto-assets and Clients' funds. The identified sources include in particular:

- **Cybersecurity**: Attempts at hacking, malware, phishing attacks or other forms of cyberattacks aimed at compromising private keys or access credentials.
- **System outages**: Unplanned outages or shutdowns of systems used for processing transactions or custody.
- **Data integrity risks:** Damage or loss of data due to system failure, software errors, or unauthorised changes.
- **Third-party risks**: Risks associated with using third-party services for custody, transaction processing or ICT infrastructure.

Management of operational and ICT risks

To manage operational and ICT risks, the Provider implements the following measures, in particular:

- **Cybersecurity Framework**: The Provider uses a multi-level cybersecurity framework that includes firewalls, intrusion detection systems and encryption protocols to protect against unauthorised access and cyberattacks.

- **Access control**: The Provider implements access control measures, including the use of hardware security modules (HSM), multi-factor authentication (MFA) and role-based access control (RBAC), to restrict access to sensitive systems and data.

- **Incident Response Plan**: The Provider has implemented an incident response plan. This plan includes predefined roles, communication strategies and recovery protocols to minimise the impact of any incident.

9 Review and audit of Client asset custody and administration policies and systems

The Provider ensures that an annual audit of the Client asset custody and administration system is conducted by an independent external auditor, in accordance with the Auditors Act. The annual audit provides independent confirmation that the Client asset custody and administration system implements appropriate measures and can withstand current threats, and that the configuration of key components meets market standards. The audit primarily focuses on the following areas:

a) the logical configuration of the wallet hierarchy;

b) security measures for working with private keys;

c) the process of managing the Provider's employee permissions.