Crypto-Asset Transfer Policy (Acting on Behalf of Clients)
Bitcan sp. z o.o.
dated 1 May 2025

I. Introduction

This Crypto-Asset Transfer Policy (Acting on Behalf of Clients) ("Policy") sets out the rules governing the provision of crypto-asset transfer services by Bitcan sp. z o.o. ("Company") on behalf of Clients, as defined in **Article 3(1)(26)** of the MiCA Regulation. The Company does not provide transfer services as a standalone crypto-asset service. It is provided exclusively in connection with another crypto-asset service. This Policy applies to all crypto-asset transfer services offered by the Company and covers every stage of the transfer process.

II. Definitions

The following definitions apply in this Policy:

- **Client** means a natural person, legal person, or other undertaking on behalf of whom the Company provides crypto-asset services.
- **Crypto-Asset** means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology (Article 3(1)(5) of the MiCA Regulation).
- **MiCA Regulation** means Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 09.06.2023, p. 40 and OJ L 2023/2869, 20.12.2023).
- **Company** means Bitcan spółka z ograniczoną odpowiedzialnością with its registered office in Poznań (60-529), ul. Jana Henryka Dąbrowskiego 77A, entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court for Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register, under KRS number: 0000808472, NIP: 6292495068, REGON: 384619443, with share capital of PLN 10,500.00.
- **Transfer** means a transaction at least partially carried out by a crypto-asset service provider on behalf of either the originator or the beneficiary, with a view to moving a crypto-asset from one distributed ledger address, crypto-asset account or crypto-asset storage device to another distributed ledger address, crypto-asset account or crypto-asset storage device, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator is the same as the crypto-asset service provider of the beneficiary (Article 3(1)(26) of the MiCA Regulation).

III. Types of Crypto-Assets for Which the Company Provides Transfer Services

The Company provides transfer services for the following crypto-assets:

- **Bitcoin (BTC)** on the **BTC network**
- **Ethereum (ETH)** on the following networks:
  - Ethereum (ERC-20); and
  - Binance Smart Chain (BEP-20)
- **Binance Coin (BNB)** on the **Binance Smart Chain (BEP-20)**

- **USD Coin (USDC)** on the following networks:
    - Ethereum (ERC-20);
    - BASE
- **ARI ($ARI)** on the **BASE network**.

IV. **Transfer Process**

For security reasons, the Company requires that crypto-asset deposits receive more than one confirmation on their respective blockchain before they can be credited to the Client's account. Confirmation requirements help prevent the risk of **double-spending**, i.e. a situation where someone attempts to use the same crypto-assets in multiple transactions.

As set out in **Table 1.0 – Crypto-Asset Transfer Conditions** (below), the Company waits for a specified number of confirmations before the crypto-assets are transferred, in order to ensure that the transaction is valid and irreversible. The more confirmations a transaction receives, the more secure it becomes. Some crypto-assets may be transferred via multiple blockchain networks. To ensure transparency, the Company always presents the available blockchain network options to the Client prior to the deposit process, allowing the Client to choose the blockchain network that best meets their needs.

Before executing a transfer, the Company warns Clients of the consequences of incorrectly specifying the network or address to which they wish to transfer assets.

Cut-Off Times

The Company establishes **cut-off times** for receiving transfer instructions. Instructions received before the designated cut-off time on a business day will be processed as received on the same day. Instructions received after the cut-off time will be processed on the next business day. Specific cut-off times are communicated to Clients and are intended to ensure timely and efficient processing of transfer requests.

Required Confirmations

The following table presents the **estimated transfer time**, assuming that the Client's transaction is confirmed in the first block after it is broadcast. If the Client's transaction is not confirmed in the first available block, the transfer may take longer depending on network conditions and the level of transaction fees.

Table 1.0 – Crypto-Asset Transfer Conditions

Crypto-Asset	Required Confirmations	Estimated Transfer Time*
Bitcoin (BTC)	1 confirmation	40 minutes; fee-dependent
Ethereum (ETH) *(Ethereum network)*	32 confirmations	14 minutes
Ethereum (ETH) *(Binance Smart Chain / BEP-20)*	32 confirmations	6 minutes
USD Coin (USDC) *(Ethereum network)*	70 confirmations	14 minutes
USD Coin (USDC) *(BASE network)*	2 blocks	5 minutes
ARI10 ($ARI) *(BASE network)*	32 confirmations	5 minutes

*Estimated time if confirmed in the next block.

Before executing a Transfer, the Company informs Clients that it has **no influence over the speed at which transactions are confirmed** on the blockchain selected by the Client.

The Company also informs Clients once the transfer has been successfully completed. The timing of such communication depends on the speed and activity level of the respective blockchain network. In extreme cases, confirmation may take several hours.

While awaiting confirmation of the successful completion of the transfer, the Company provides the Client with **ongoing updates** regarding the status of their transaction.

V. Client Information Principles

1. Information Provided Before the Commencement of the Transfer Service

Before commencing the provision of the Transfer service, the Company shall provide the Client, in a clear and comprehensible manner and using plain language, with the following information:

- the name of the Company, the address of its registered office, and any other addresses and means of communication, including email address, relevant for communication with the Company;
- the name of the competent national authority responsible for supervising the Company;
- a description of the main characteristics of the Transfer service to be provided;
- a description of the form and procedure for initiating the Transfer or giving consent thereto, and for withdrawing the instruction or consent, including details of the information the Client must provide to properly initiate or execute the Transfer (including authentication methods);
- the conditions under which the Company may refuse to execute a Transfer instruction;
- a reference to the procedure or process established by the Company for determining the time of receipt of the Transfer instruction or consent to the transfer of crypto-assets, and any cut-off times established by the Company;
- with respect to each specific crypto-asset – an explanation of the distributed ledger technology (DLT) network supported for the transfer of that crypto-asset;
- the maximum execution time for the Transfer service to be provided;
- for each DLT network – a reasonably estimated time or number of block confirmations required for the transfer to be irreversible, or considered sufficiently irreversible in the case of probabilistic settlement, taking into account the rules and circumstances of the DLT network;
- all fees and charges payable by the Client in connection with the Transfer service, including any fees related to the method and frequency of providing or making available the information, and – where applicable – a breakdown of such charges;
- the means of communication, including basic information about the technical requirements concerning the Client's hardware and software (e.g. minimum software or mobile operating system) as agreed between the parties for the transmission of information or notifications related to the Transfer service;
- the manner and frequency of providing or making available information related to the Transfer service;
- a secure procedure for notifying the Client in the event of suspected or actual fraud or a security threat;

- the means and timeframe within which the Client is required to notify the Company of any unauthorised or incorrectly initiated or executed Transfers, and the Company's liability – including the maximum amount – for such unauthorised or incorrect Transfers;
- the Client's right to terminate the Transfer service agreement and the procedures for doing so.

The above information is provided to Clients free of charge in electronic form. It is also made available in a format that allows the Client to store and reproduce it unchanged. The Company shall inform the Client in advance of any changes to the above information before such changes become effective.

2. **Information Provided Before the Execution of the Transfer**

Immediately before executing the Transfer, the Company informs the Client whether and when the crypto-asset transfer will be irreversible, or sufficiently irreversible in the case of probabilistic settlement. Additionally, the Company informs the Client of any applicable fees, and, where applicable, provides a breakdown of the amounts due, distinguishing between fees charged for the transaction via the relevant DLT network and any other fees charged by the Company for the provision of services.

3. **Information Provided After the Execution of the Transfer**

After the successful execution of the Transfer, the Company provides the Client with the necessary information. In particular, the Company provides the following information related to the Transfer:

- the name of the originator and the beneficiary of the Transfer;
- the distributed ledger address or crypto-asset account number of the originator of the Transfer;
- the distributed ledger address or crypto-asset account number of the beneficiary of the Transfer;
- a reference number enabling the Client to identify each Transfer;
- the amount and type of crypto-assets transferred or received in the Transfer;
- the value date applied to the debit or credit related to the Transfer;
- the amount of any fees or charges related to the Transfer and – where applicable – a breakdown of such amounts.

The Company makes the Transfer history available to Clients for a period of **one year** from the date of each transaction via information provided on the Company's Website. After this one-year availability period, the transaction history will no longer be available by default but may be provided to the Client or a third party if required by applicable legal or regulatory obligations.

4. **Information Provided in Case of Rejection, Return, or Suspension of a Transfer**

In the event of a **rejection, return, or suspension** of a Transfer, the Company provides the Client with the following information:

- the reason for the rejection, return, or suspension;
- where applicable – information on how to resolve the issue that led to the rejection, return, or suspension;
- the amount of any fees or charges incurred by the Client and information on whether such amounts are refundable.

5. **Additional Information Provided to Clients**

The Company provides Clients with information on the **measures implemented to protect their assets**, including the technological solutions used by the Company.

Any changes to transfer procedures or risk mitigation strategies are communicated to Clients via email or published on the Company's Website.

Additionally, Clients have access to **educational materials** available on the Company's Website, which explain the potential risks associated with Transfers.

The Company also maintains a **Client Support Team**, whose role is to provide Clients with information and assistance related to the Transfer process.

VI. **Form of Information Provision**

All information referred to in this Policy is provided to Clients **free of charge** in **electronic form**. The Company may establish appropriate fees for the provision of such information, in accordance with the rules arising from applicable legal provisions.

VII. **Transfer-Related Information**

In order to execute a Transfer, the Company obtains from the Client a set of information that enables the identification of both the **originator** of the given Transfer (i.e. the Client) and its **beneficiary** (i.e. the recipient of the Transfer).

When executing a Transfer, the Company ensures that it is accompanied by the following data about the **Client**:

- the **full name** or – where the Client is not a natural person – the **name of the Client**;
- the **distributed ledger address** of the Client, where the Transfer is recorded on a DLT network or similar technology, and the Client's **crypto-asset account number**;
- the Client's **crypto-asset account number**, where the Transfer is not recorded on a DLT network or similar technology;
- the **Client's address**, including country, official identity document number, and Client identification number or – alternatively – the Client's **date and place of birth**;
- the **current LEI** (Legal Entity Identifier), where a corresponding field exists in the applicable payment message format and the Client has provided such identifier to the Company, or – in the absence thereof – any other available equivalent official identifier of the Client.

The Company also ensures that the following data about the **beneficiary** accompanies the Transfer:

- the **full name** or – where the beneficiary is not a natural person – the **name of the beneficiary**;
- the **distributed ledger address** of the beneficiary, where the Transfer is recorded on a DLT network or similar technology, and the **beneficiary's crypto-asset account number**;
- the **current LEI** of the beneficiary, where a corresponding field exists in the applicable payment message format and the Client has provided such identifier to the Company, or – in the absence thereof – any other available equivalent official identifier of the beneficiary.

In cases where the Transfer is **not recorded** on a DLT network or similar technology, and **not executed to or from a crypto-asset account**, it is possible that instead of the originator's and beneficiary's crypto-asset account numbers, the Transfer is accompanied by a **unique transaction identifier**.

The Transfer-related information referred to in this section must be provided to the Company by the Client **no later than at the moment of executing the Transfer**. This information does not have to be embedded directly in the Transfer itself.

Where the Transfer is made to an **unhosted address**, the Company obtains and stores the Transfer-related information and ensures the **individual traceability** of the Transfer.

For any Transfer **exceeding the equivalent of EUR 1,000** to an unhosted address, the Company shall take **appropriate measures to assess** whether such an address is owned or controlled by the Client.

Before executing a Transfer, the Company verifies the **accuracy** of the information mentioned above. If the above requirements are not met, the Company shall request the Client to **provide or correct** the information. If the information is not provided or is provided incorrectly, the Company shall **not execute the Transfer** and shall exercise due diligence to return the Client's funds in accordance with the **Terms of Service**. Once any concerns are resolved, the Company will proceed with the Transfer

VIII. **Persons Responsible for Transfers**

Within the Company, there is a **dedicated Transfer Team** responsible for monitoring and overseeing Transfers. As part of its responsibilities, the team is in charge of:

- processing and executing Transfers, ensuring their **accuracy**, **compliance**, and **timely execution**;
- conducting **ongoing risk assessments**, with a focus on operational failures, cybersecurity risks, and **compliance with the MiCA Regulation**;
- ensuring **prompt response** in the event of system failures or breaches of security protocols;
- approving Transfers that are classified as **non-standard** or that **exceed thresholds** defined in the Company's internal policies.

The approval of non-standard Transfers is carried out in accordance with the **principle of segregation of duties**.

IX. Risk Management and Business Continuity with Respect to Transfers

1. **ICT Systems Supporting Risk Management**

The Company has implemented the following ICT systems and functionalities to support risk management in the context of Transfers:

- **Automated monitoring systems**: The Company uses ICT systems that monitor Transfers and detect operational anomalies or potential cybersecurity threats. Automated alerts are triggered to enable immediate action and incident analysis.
- **Redundancy and data backups**: The Company maintains redundant systems and creates regular data backups to prevent service disruptions and ensure continuity of transfer services.

- **Use of MPC (multi-party computation) wallets**: The MPC private key protection layer eliminates any single point of compromise, both from internal and external threats, as the private key is never stored on a single device at any time.
- **Enforced multi-person approval**: Operations involving wallets or non-standard activities always require confirmation by more than one person.

2. **Persons Responsible for Risk Management**

Responsibility for managing Transfer-related risk lies with the **Management Board** of the Company. The **dedicated Transfer Team** includes cybersecurity specialists tasked with identifying vulnerabilities in transfer processes and implementing protections against potential attacks. The Transfer Team receives **regular training** on emerging threats, new regulatory requirements under MiCA, TEFR, and **Regulation (EU) 2022/2554** of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

3. **Incident Management**

In the event of a **high-risk incident**, the Company applies an **escalation procedure** to immediately inform the Management Board and relevant staff members. Clients are promptly notified of the incident and informed of the steps taken to resolve the issue and mitigate its impact. The Company follows **strict incident response timelines**, providing Clients with a clear recovery plan and estimated resolution time.

4. **Business Continuity Procedure**

The Company has implemented a **Business Continuity Plan (BCP)** to ensure the uninterrupted provision of Transfer services even in the case of unexpected events such as system failures or cyberattacks. The plan includes, among other measures:

- regular **disruption simulation exercises** to test digital resilience and staff readiness;
- functioning **backup systems** to minimise downtime and ensure rapid service recovery in case of disruptions;
- storing only the amount of crypto-assets necessary for operational purposes in a **hot wallet**. The remaining assets are stored in a secure **cold wallet**, i.e., a hardware crypto-asset wallet.

X. **Company Liability**

The Company shall be liable to the Client for any unauthorised or incorrectly initiated or executed Transfers **only for losses or damages** it is required to cover under **applicable local consumer protection laws**.

XI. **Registration and Audit of Transfer Services**

1. **Transfer Services Register**

The Company maintains an **internal register of crypto-asset transfer services** provided on behalf of Clients, which includes at a minimum:

- the date and time of receipt of the transfer instruction;
- the date and time of the transfer execution;
- the crypto-asset addresses of the originator and the beneficiary;

- the transaction identifier (e.g., hash, reference number);
- the type and value of the crypto-asset transferred;
- the DLT (blockchain) network used;
- information on fees charged to the Client;
- the execution status of the transfer and, where applicable, the reason for rejection, return, or suspension of the transfer.

2. **Data Retention Period**

The data contained in the register shall be retained for the period required under applicable laws, in particular laws on the **prevention of money laundering and terrorist financing**, and **accounting documentation retention requirements**, but **no less than five (5) years** from the date of the respective transfer.

3. **Internal and External Audit**

The Company ensures the ability to conduct **regular internal audits**, and, where necessary, **external audits**, to verify compliance of the transfer service with applicable laws, this Policy, and the Company's internal regulations.

The audit specifically covers:

- the effectiveness of transfer monitoring and control systems;
- the compliance of the identification data of originators and beneficiaries with legal requirements;
- the completeness and accuracy of the transfer register;
- the observance of the Client information principles.

4. **Audit Documentation**

Audit results are documented in written form and submitted to the Company's Management Board. In the event of any identified irregularities, corrective actions are undertaken in accordance with the Company's internal incident and non-compliance management procedure.

5. **Cooperation with Supervisory Authorities**

The Company ensures access to the transfer register and audit documentation upon request from the competent supervisory authority, or the supervisory authority of another Member State of the European Union, to the extent falling within their jurisdiction.

XII. **Review of this Policy**

This Policy is subject to **annual review**, as well as review in the event of significant changes in the Company's organisational structure **or** material legal developments**.** Any amendments to this Policy are subject to approval by the Company's Management Board**.**