CUSTODY AND ADMINISTRATION AGREEMENT

CODESPRINGCZ S.R.O.

DRAFT FOR REGULATORY SUBMISSION – ARTICLE 62(2)(M) MICA

BOARD MEMBER: SERGEI TOROPTSEV

WEBSITE: HTTPS://CODE-SPRING.EU

REGISTERED ADDRESS: KURZOVA 2222/16, 155 00, PRAHA 5 - STODŮLKY, CZECH REPUBLIC

COMPANY ID (IČO): 22402012

CUSTODY AND ADMINISTRATION AGREEMENT

This Custody and Administration Agreement is made and entered into on this DATE (the “Effective Date”), by and between:

CodeSpringCZ s.r.o., a limited liability company duly incorporated and existing under the laws of the Czech Republic, with its registered office at Chudenická 1059/30, 102 00 Praha 10 – Hostivař, Czech Republic, registered in the Czech Commercial Register maintained by the Municipal Court in Prague, Company ID (IČO): 22402012, authorised to provide crypto-asset services pursuant to **Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)**, (hereinafter referred to as the “**Service Provider**”),

and

[Client’s Full Legal Name], a [natural person] residing under the laws of [jurisdiction], with its residential address at [Insert Address], Personal ID: [Insert], (hereinafter referred to as the “**Client**”),

(each individually a “**Party**” and collectively the “**Parties**”).

1. Purpose and Scope

1.1. The purpose of this Agreement is to establish the terms and conditions under which **CodeSpringCZ s.r.o.** (the “Service Provider”) shall provide custody and administration services of crypto-assets to the Client, in strict compliance with **Article 75 of Regulation (EU) 2023/1114 on Markets in Crypto-Assets (“MiCA”)**, related implementing measures, and applicable Czech national legislation.

1.2. The scope of this Agreement expressly covers the safekeeping, recording, and administration of crypto-assets belonging to the Client, including but not limited to:

- the maintenance of crypto-assets in wallets or accounts under the control of the Service Provider;
- the management of cryptographic keys necessary for the secure storage and transfer of such assets;
- the facilitation of transfers and withdrawals on the Client’s instructions; and
- the protection of the Client’s ownership rights at all times.

1.3. The Service Provider undertakes to perform its obligations with a standard of professional care consistent with recognised industry best practices, taking into account the evolving nature of distributed ledger technology (“DLT”) and the heightened need for robust cybersecurity and operational safeguards.

1.4. In line with **Article 75(1) MiCA**, this Agreement constitutes a legally binding arrangement between the Service Provider and the Client that ensures clarity of rights and obligations, transparency of procedures, and enforceability of the Client's entitlements with respect to their crypto-assets. The Service Provider further confirms that it has established a **summary custody policy**, which will be made available to the Client, detailing the safeguarding principles, internal governance, and risk controls applicable to the custody services.

1.5. The custody services provided hereunder shall be carried out exclusively in the Client's interest, with full recognition that the Client remains the ultimate and beneficial owner of the crypto-assets at all times. The Service Provider shall not, under any circumstances, use, pledge, rehypothecate, or otherwise encumber the Client's crypto-assets for its own account or for the account of third parties, except where explicitly authorised by the Client in writing and permitted by law.

1.6. The scope of custody and administration includes both **segregated custody arrangements** (where assets are held in wallets designated solely for a particular Client) and **omnibus custody arrangements** (where assets of multiple clients are pooled in a single wallet, with internal records clearly allocating ownership rights). The Service Provider commits to ensuring that its accounting and recordkeeping systems are sufficiently detailed, accurate, and auditable so that each Client's holdings can be identified without ambiguity at any given time.

1.7. In accordance with **Article 75(8) MiCA**, the Service Provider shall adopt measures to:

- respect the Client's rights in relation to the crypto-assets held in custody;
- segregate the Client's crypto-assets from those of the Service Provider and from other clients, unless omnibus custody has been contractually agreed;
- maintain robust operational and ICT risk management controls to safeguard assets against theft, cyber-attacks, or unauthorised access; and
- provide regular and transparent reporting to the Client regarding the balance, movement, and status of their assets.

1.8. The Service Provider acknowledges that its custodial role carries significant responsibilities toward both the Client and the wider financial ecosystem. Consequently, it shall ensure that its custody and administration activities are consistent with **the prudential standards under Title VI of MiCA**, the relevant provisions of the **Digital Operational Resilience Act (DORA)**, and applicable Czech laws on financial supervision, insolvency, and consumer protection.

1.9. The Parties acknowledge that this Agreement is not intended to transfer ownership of the crypto-assets to the Service Provider but merely to establish a fiduciary-type custody relationship, whereby the Service Provider safeguards, administers, and facilitates transactions strictly on behalf of the Client.

1.10. This Agreement applies to all custody and administration services provided by the Service Provider as of the effective date, and shall continue to govern such services until terminated in accordance with the provisions herein. The Service Provider reserves the right to enhance its custody framework from time to time in response to regulatory updates, technological developments, or supervisory requirements, provided that such enhancements do not adversely affect the Client’s rights or diminish the level of protection afforded under this Agreement.

2. Type of Custody

2.1. **Segregated Custody**

The Service Provider offers the option for the Client’s crypto-assets to be held in **individual wallets** that are fully segregated from:

- the Service Provider’s own assets; and
- the assets of any other client.

This model ensures the **highest level of legal and operational protection**, as ownership and entitlement to the assets remain clearly attributable to the Client at all times. Segregated custody minimises legal and insolvency risks, ensuring that, in the unlikely event of the Service Provider’s insolvency, the Client’s assets shall not form part of the Service Provider’s estate but shall remain the Client’s sole property, in full compliance with **Article 75(7) of MiCA**.

2.2. **Omnibus Accounts**

In certain circumstances, the Service Provider may hold crypto-assets of multiple clients in a **common wallet (omnibus account)** for efficiency and operational flexibility. In such cases, the Service Provider shall maintain **detailed internal records and reconciliation processes** on a continuous basis, enabling the accurate allocation of each client’s entitlements.

The Service Provider undertakes to:

- maintain **daily reconciliations** between on-chain balances and internal records,
- implement robust **accounting and ledger systems** ensuring a clear mapping between omnibus holdings and individual client entitlements, and
- ensure that omnibus custody arrangements are operated with the **same level of legal protection** as segregated accounts, in accordance with Article 75 MiCA.

The Client acknowledges and agrees that omnibus custody may carry certain risks, including potential delays in asset recovery in case of insolvency proceedings. These risks are mitigated by the Service Provider’s strict adherence to prudential requirements, insurance coverage, and internal control mechanisms.

2.3. Cryptographic Key Management

The Service Provider shall manage **private and public cryptographic keys** associated with the Client’s assets under the highest standards of security and governance. This includes, without limitation:

- **multi-signature protocols** and role-based access controls,
- **encryption at rest and in transit**,
- **geographically distributed cold storage** for long-term asset security,
- continuous **monitoring and incident detection systems**, and
- regular **penetration testing and threat simulations**.

The Service Provider’s key management framework is fully aligned with **MiCA, the Digital Operational Resilience Act (DORA), and international standards such as ISO/IEC 27001**.

2.4. Client Instructions and Transparency

All custody arrangements shall be executed strictly in accordance with the Client’s instructions and in line with applicable law. The Service Provider shall provide the Client with **regular statements and reports** evidencing the safekeeping of assets, wallet balances, and transaction history.

3. Instruments of Constitution and Governing Framework

The incorporation and governance framework of **CodeSpringCZ s.r.o.** is established in full compliance with the **laws of the Czech Republic** and the **requirements of Regulation (EU) 2023/1114 (MiCA)**. The Company was duly incorporated by **notarial deed** and is registered in the **Czech Commercial Register maintained by the Municipal Court in Prague**.

The Company’s **instruments of constitution** — including the Founding Deed and Articles of Association — establish the legal foundation of its activities, governance, and internal control mechanisms. Together, they provide a transparent and enforceable framework for management, shareholder rights, and compliance obligations under EU and Czech law.

In line with **Article 62(2)(c) of MiCA**, certified copies of these documents are attached to the present application, together with an official extract from the Commercial Register confirming their validity.

3.1 Founding Deed

The **Founding Deed** of CodeSpringCZ s.r.o. serves as the primary constitutive document of the Company. Executed before a Czech notary in accordance with **Act No. 90/2012 Coll., on Commercial Companies and Cooperatives (Business Corporations Act)**, it sets forth:

- the legal form of the Company as a **limited liability company (společnost s ručením omezeným)**;
- the registered corporate name and seat of the Company;
- the scope of business activities, including services subject to **MiCA authorisation** (custody and administration of crypto-assets on behalf of clients, and exchange of crypto-assets for funds or other crypto-assets);
- the amount of registered capital and shareholder contributions;
- the structure of corporate governance and representation.

The Founding Deed ensures that the Company is endowed with the necessary **legal personality**, thereby guaranteeing enforceability of obligations, proper allocation of liability, and safeguarding of clients' rights in accordance with Czech corporate law.

3.2 Articles of Association

The **Articles of Association** of CodeSpringCZ s.r.o. provide a comprehensive framework for the Company's governance and internal functioning. They define:

- **governance structure** (statutory body, shareholders' meeting, internal functions);
- **management duties**, including compliance with obligations under **MiCA and Czech AML legislation (Act No. 253/2008 Coll.)**;
- **shareholder rights and obligations**, including voting rights, dividend entitlements, and procedures for capital changes;
- **internal decision-making rules**, ensuring proper checks and balances in risk-sensitive operations such as custody and exchange of crypto-assets;
- **appointment of compliance and risk functions**, in particular the designation of an **AML/CTF officer (MLRO)** and compliance officer, aligned with MiCA Article 61 and Czech AML law.

The Articles also provide explicit safeguards to ensure **segregation of client assets from the Company's own funds** and mandate compliance with prudential requirements under **MiCA Article 67**.

3.3 By-Laws and Internal Rules

In addition to the Founding Deed and Articles of Association, the Company has adopted a set of **internal by-laws and policies** that operationalise its governance framework. These include:

- **AML/CTF Compliance Policy**, setting out internal control systems and reporting channels;
- **ICT and Cybersecurity Policy**, aligned with **MiCA Title VII and DORA**, addressing operational resilience and incident management;
- **Risk Management Policy**, covering prudential, operational, and market risks;
- **Conflict of Interest Policy**, ensuring transparency and fair treatment of clients in line with MiCA Article 72;

- **Whistleblowing Procedure**, guaranteeing anonymous reporting of misconduct, in line with Article 61(2) MiCA and Czech Act No. 171/2023 Coll.

These internal rules are binding on the Company's management and staff, forming part of the broader **compliance and governance architecture** required for authorisation under MiCA.

3.4 Supporting Documentation

As supporting documentation to this application, the following certified copies and extracts are enclosed:

1. **Founding Deed of CodeSpringCZ s.r.o.** executed before a Czech notary.
2. **Articles of Association** setting out the Company's internal governance rules.
3. **Extract from the Czech Commercial Register**, evidencing incorporation and current status.
4. **Internal By-Laws and Policies**, including AML/CTF, Risk Management, ICT, and Compliance frameworks.

4. Address of the Head Office and Registered Office

In accordance with **Article 62(2)(d) of Regulation (EU) 2023/1114 (MiCA)**, the applicant, **CodeSpringCZ s.r.o.**, hereby confirms the location of its head office and registered office.

The Company's **head office and registered office** are situated at the following address:

CodeSpringCZ s.r.o.
Kurzova 2222/16
155 00, Praha 5 – Stodůlky
Czech Republic

Both the **head office** and **registered office** are located at the same address, ensuring administrative and operational centralisation. The premises serve as the Company's **legal seat**, as duly recorded in the Czech Commercial Register maintained by the Municipal Court in Prague, and as the **principal place of management and decision-making**.

The registered office is fully compliant with the requirements of the **Business Corporations Act (Act No. 90/2012 Coll.)**, which obliges Czech companies to maintain a clearly defined and verifiable legal seat. All statutory correspondence, regulatory notifications, and official communications from the **Czech National Bank (CNB)** and other competent authorities are duly received at this address.

From an operational standpoint, the head office functions as the Company's **core administrative centre**, where:

- governance and management activities are carried out by the statutory body;
- internal policies and compliance functions (AML/CTF, ICT risk management, and prudential safeguards) are coordinated;
- records required under **MiCA Article 61(5)** and **Czech AML legislation** are securely maintained;
- client-facing operations (custody and exchange of crypto-assets) are overseen and controlled.

At the current stage, CodeSpringCZ s.r.o. does **not maintain any additional offices, branches, or permanent establishments** in other EU Member States or third countries. The Company's operations are centralised in Prague, ensuring **efficient oversight, cost-effectiveness, and regulatory transparency**.

The Company further undertakes that any future changes to its registered office, establishment of branches, or operational relocation within or outside the Czech Republic will be **immediately notified to the Czech National Bank** in accordance with applicable law and supervisory requirements.

5. Fees and Charges

In accordance with the principles of **fairness, transparency, and disclosure** set out under **Article 62(2) of Regulation (EU) 2023/1114 (MiCA)** and applicable consumer protection provisions under **Czech law**, the applicant, **CodeSpringCZ s.r.o.**, hereby sets out its fee structure relating to the provision of custody and administration of crypto-assets on behalf of clients and the exchange of crypto-assets for funds or other crypto-assets.

The Company's approach to fees is based on the following principles:

- **Transparency** – all fees and charges are disclosed to clients in advance of service provision, in a clear and comprehensible manner, avoiding hidden or misleading costs.
- **Fairness and proportionality** – fees are determined in line with the value of services provided, the risk profile of the transaction, and market practice in the Czech Republic and the European Union.
- **Predictability** – clients are provided with a full overview of applicable charges prior to entering into a contractual relationship, ensuring that no unforeseen or disproportionate costs arise.
- **Regulatory compliance** – the fee schedule is prepared in full compliance with **MiCA** and other relevant European and Czech legislation, including obligations to disclose all costs to natural persons in plain and non-technical language.

5.1 CUSTODY AND ADMINISTRATION FEES

The Client shall pay custody and administration fees as set out in **Schedule A (Fee Schedule)**. These fees cover the safeguarding, monitoring, and administrative handling of clients' crypto-assets, including the execution of rights associated with such assets. Fees may be structured on the basis of:

- a **fixed monthly or annual service fee**;
- a **percentage fee based on the value of the assets under custody**; or
- a **transactional fee** for specific events, such as withdrawals, transfers, or execution of client instructions.

5.2 EXCHANGE SERVICE FEES

For services falling under **Article 77 MiCA** (exchange of crypto-assets for funds or other crypto-assets), the Company shall apply clearly defined fees, including:

- **conversion spreads** on exchange rates;
- **transaction-based commissions**; and
- where applicable, **network or blockchain-related charges**, passed on transparently to the client without additional mark-ups.

5.3 DISCLOSURE OF FEES

All fees are communicated to clients in writing prior to the commencement of services, in the form of:

- a **Fee Schedule** annexed to the client agreement;
- upfront disclosure during the client onboarding process; and
- ongoing access to the Fee Schedule through the Company's official website.

Clients are further informed of their right to request clarifications at any stage. Any modification of the Fee Schedule will be subject to **prior notification** to clients, ensuring a reasonable period for review before implementation.

5.4 PROHIBITION OF HIDDEN CHARGES

The Company explicitly confirms that **no hidden charges, retroactive costs, or undisclosed mark-ups** will be applied. All charges must be justified, disclosed, and aligned with the service provided.

5.5 SUPERVISORY OVERSIGHT

In compliance with **MiCA** and **Czech consumer protection rules**, the Company undertakes to:

- maintain its Fee Schedule under continuous review to ensure market fairness;
- notify the **Czech National Bank (CNB)** of any significant changes affecting the structure or level of client charges, if required; and

- preserve records of all communications relating to fees, in line with **MiCA Article 61(5)** record-keeping requirements.

6. Liability and Risk Allocation

6.1. The Service Provider shall be liable towards the Client for direct losses demonstrably arising from the Service Provider's gross negligence, fraud, or willful misconduct in the safekeeping, administration, or return of the Client's crypto-assets. Liability shall be determined in accordance with applicable provisions of Czech law and Regulation (EU) 2023/1114 (MiCA).

6.2. The Service Provider shall not be liable for indirect or consequential damages, including but not limited to loss of profit, loss of opportunity, or reputational damage, except where such damages result from fraud or willful misconduct.

6.3. The Service Provider shall not be liable for losses caused by:
(a) market risks inherent to the volatility of crypto-assets;
(b) systemic failures of blockchain protocols or distributed ledger technology on which the relevant crypto-assets rely;
(c) cyber-attacks, hacking, or external malicious actions that occur despite the Service Provider's implementation of state-of-the-art security measures and industry-standard safeguards;
(d) regulatory changes or force majeure events beyond the Service Provider's reasonable control.

6.4. The Parties expressly agree that the Client bears the investment risk associated with crypto-assets, and that the Service Provider's liability is strictly limited to custodial and administrative functions as described in this Agreement.

7. Return of Assets

7.1. The Service Provider shall, upon the Client's written request, return the Client's crypto-assets or the cryptographic means of access to such assets without undue delay, provided that the Client has complied with all obligations under this Agreement and subject to the completion of appropriate security, compliance, and anti-money laundering (AML/CTF) checks.

7.2. In the event of termination of this Agreement, the Service Provider shall, within a commercially reasonable period, transfer all Client-owned assets to a digital wallet designated by the Client. Such transfer shall be performed only after due verification of the designated wallet, the Client's identity, and any other regulatory requirements applicable under Czech law and MiCA.

7.3. The Service Provider shall not retain, pledge, or otherwise encumber the Client's assets except where required by law or expressly agreed in writing by the Parties.

7.4. The Client acknowledges that technical delays inherent to blockchain settlement mechanisms may affect the speed of transfers and agrees that the Service Provider shall not be liable for delays caused by blockchain congestion or failures outside its direct control.

8. Insurance and Safeguards

8.1. The Service Provider may maintain an insurance policy to cover certain risks associated with the custody and administration of crypto-assets, including theft, fraud, operational failures, and cybersecurity incidents. The scope, coverage limits, and exclusions of such insurance shall be communicated to the Client upon request.

8.2. The Service Provider shall implement and regularly update a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) designed to ensure ongoing availability of assets, continuity of critical operations, and protection of client assets against loss or unauthorized access.

8.3. The Service Provider shall also maintain internal security and risk management systems proportionate to the scale and complexity of its operations, in accordance with Article 67 and Article 75(8) of Regulation (EU) 2023/1114, and aligned with international standards of cybersecurity and operational resilience.

8.4. The Client acknowledges that no insurance or safeguard can fully eliminate all risks inherent in holding or transferring crypto-assets.

9. Term and Termination

9.1. This Agreement shall enter into force on the Effective Date and shall remain valid for an indefinite duration unless terminated in accordance with the provisions herein.

9.2. Either Party may terminate this Agreement at any time by providing the other Party with not less than thirty (30) calendar days' prior written notice, unless a different period is mutually agreed in writing.

9.3. The Service Provider shall have the right to terminate this Agreement with immediate effect in the event that:
(a) the Client breaches applicable laws or regulations, including but not limited to AML/CTF requirements;
(b) the Client provides false, misleading, or incomplete information in connection with this Agreement;
(c) the Client becomes insolvent, enters bankruptcy, or is otherwise unable to meet its financial obligations;
(d) continued provision of services to the Client would expose the Service Provider to regulatory, reputational, or legal risks.

9.4. Upon termination, the Service Provider shall return all Client assets in accordance with Chapter 7, subject to applicable legal and compliance requirements.

10. Governing Law and Jurisdiction

10.1. This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of the Czech Republic and applicable European Union legislation, including Regulation (EU) 2023/1114 (MiCA).

10.2. Any disputes arising under or in connection with this Agreement shall be submitted to the exclusive jurisdiction of the competent courts in Prague, Czech Republic, unless the Parties mutually agree to arbitration or another dispute resolution mechanism.

10.3. The Parties agree that this jurisdiction clause reflects their express and informed choice, ensuring predictability and consistency in dispute resolution.

12. Execution and Signatures

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed in two (2) originals, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

This Agreement enters into force on the date of the last signature affixed below ("Effective Date").

CodeSpringCZ s.r.o.

Board Member: Sergei Toroptsev

COMPANY ID (IČO): 22402012

Client's name

Address of residence:

Document number: