Summary of the Fiduciary Policy of Ilirika d.d. Ljubljana

ILIRIKA

ILIRIKA borzno posredniška hiša d.d., Ljubljana
Slovenska cesta 54 A, 1000 Ljubljana, Slovenija

Tel + 386/1/300 22 50
www.ilirika.si, info@ilirika.si

ILIRIKA borzno posredniška hiša d.d., Ljubljana
Slovenska cesta 54 A, 1000 Ljubljana, Slovenija
Tel + 386/1/300 22 50, fax + 386/1/234 33 57
www.ilirika.si, info@ilirika.si

SUMMARY OF THE FIDUCIARY POLICY OF ILIRIKA D.D. LJUBLJANA

Contents

I. Overview

This summary of the custody policy ("summary") describes the procedures and controls implemented by ILIRIKA borzno posredniška hiša d.d., Ljubljana, Slovenska cesta 54a, 1000 Ljubljana (hereinafter: ILIRIKA or the company or custodian) for the custody and management of crypto assets on behalf of clients, and may be provided to clients at their express request within the meaning of Article 75 of Regulation (EU) 2023/1114 on markets in crypto assets (hereinafter MiCA).

In accordance with MiCA, "providing custody and management of crypto-assets on behalf of clients" means holding or controlling crypto-assets or means of access to crypto-asset property on behalf of clients, where applicable in the form of private keys.

ILIRIKA acts as a custodian for its clients and provides them with crypto asset custody and wallet services directly. Therefore, the company acts as a contractual party for custody services in relation to its clients and assumes responsibility for the storage and custody of its clients' crypto assets ("custodian").

II. Custody partners

Custody services for all cold, warm and hot wallets are provided by a third-party custody service provider acting as a sub-custodian, which also provides the wallet infrastructure or is a technology provider.

In accordance with Article 75(9) of MiCA, if crypto-asset service providers that provide custody and management of crypto-assets on behalf of clients use other service providers, they may only use crypto-asset service providers that are authorised in accordance with Article 59 of MiCA.

ILIRIKA provides crypto-asset custody and management services (hereinafter: custody services) in accordance with the ninth paragraph of Article 75 of MiCA through the sub-custodian of Boerse Stuttgart Digital Custody GmbH (hereinafter: BSDC or sub-custodian), which holds a valid licence to provide custody and management services for clients' crypto assets (in German: *Kryptoverwahrer)*. by the competent authority of the German Financial Supervisory Authority Bafin . BSDC is a member of the Stuttgart Stock Exchange Group.

BSDC acts as a sub-custodian for cold, warm and hot wallets and also provides software technologies. For reasons of efficiency and to exploit synergy effects, certain operational and regulatory services are provided by internal service providers of the Stuttgart Stock Exchange Group and external sub-custodian providers.

When trading via the Bitstamp crypto asset trading platform, customer crypto assets are stored with Bitstamp's sub-custodian, BitGo Europe GmbH, which manages the technical infrastructure where customer crypto assets are stored. Bitstamp has a valid licence to provide custody and management services for customer crypto assets from the competent authority, the Luxembourg supervisory authority CSSF, in accordance with the provisions of MiCA. BitGo Europe GmbH holds a valid licence to provide custody and management services for clients' crypto assets from the competent authority, the German Financial Supervisory Authority (BaFin), in accordance with the provisions of MiCA.

The custodian is a provider of investment services and services related to crypto assets, supervised by the SECURITIES MARKET AGENCY, Poljanski nasip 6, 1000 Ljubljana (hereinafter: ATVP) and is authorised to provide custody and management services for crypto assets in accordance with point (a) of the third paragraph of Article 60 of MiCA.

III. Nature of omnibus (collective) accounts

a. Omnibus account

ILIRIKA has a joint (omnibus) cryptocurrency wallet opened with BSDC or Bitstamp on the basis of a concluded contract, which has the characteristics of a joint (omnibus) account (omnibus account) on which ILIRIKA jointly manages the crypto assets of clients in the form of individual crypto assets in its own name and on behalf of clients (hereinafter: omnibus account). The omnibus account is used for the

joint storage of crypto assets of multiple clients. ILIRIKA does not store its own crypto assets in the omnibus account. The company stores crypto assets in its own name and on behalf of its clients in this omnibus account.

In technical terms, the collective account is a custodial wallet on the blockchain, where private keys are managed by BSDC. Clients' crypto assets in this wallet are separate from the company's crypto assets and protected from creditors in the event of insolvency proceedings against the company and this contractual partner (bankruptcy remote on-chain wallet).

The collective account stores clients' crypto assets and also trades in crypto assets. Trading is conducted in such a way that sell and buy orders submitted to ILIRIKA via interfaces (API) are redirected to BSDC, which executes the orders through its contractual partners and arranges all necessary relations with them regarding the execution of individual orders. In this way, BSDC assumes the counterparty risk in trading. Settlement of transactions is carried out internally on a net basis.

In the case of trading via the Bitstamp trading platform, ILIRIKA directly executes sell and buy orders in its own name and on behalf of the client (indirect representation).

Hereinafter, Bitstamp and BSDC are also jointly referred to as sub-custodians.

b. Internal records

The records and separate management of clients' crypto assets in the collective account are provided by ILIRIKA's internal IT support and software, namely the Shark application (hereinafter: crypto asset account), which shows at any given moment which crypto assets in the collective account belong to individual clients.

ILIRIKA concludes a written contract with the client for the custody and management of crypto assets, on the basis of which ILIRIKA, in return for a commission, stores the clients' crypto assets with the custodian in a joint account. This is an integrated custody and trading service, where the contractual partner is solely a regulated counterparty (i.e. BSDC or Bitstamp).

IV. Monitoring the wallet balance

As best practice and to reduce risks, ILIRIKA stores most of its clients' crypto assets offline in cold wallets. The value of crypto assets in cold wallets is monitored daily.

V. Separation between clients' crypto assets and the custodian's own assets

VI. Actual separation

The custodian does not store its own crypto assets in a collective account. Crypto assets owned by clients are always considered to belong to the client who owns the crypto assets.

Clients' crypto assets are stored together in a collective account. Clients' crypto assets are held in the name of the custodian and for the account of the clients.

The custodian's internal accounting system (Shark application) is used to assign ownership of the crypto assets in the collective account to the clients. The custodian does not use the clients' crypto assets for other purposes, such as lending or pledging, without their consent. In the event of the custodian's insolvency, the clients' crypto assets are credited to the client so that the insolvency administrator can exclude them from the custodian's insolvency estate.

VII. Legal separation

Clients are the legal owners of the crypto assets held by the custodian in a collective account in its own name and on behalf of its clients.

Given the special nature of crypto assets, custody of crypto assets consists of the storage of confidential private keys for crypto assets. ILIRIKA does not have, and the parties agree that ILIRIKA does not have and will not acquire, any rights, ownership or share in the crypto asset property held on behalf of the parties.

VIII. Ensuring separation of assets in the event of insolvency

Cryptocurrencies held in custody are legally separated from the company's assets in accordance with applicable law, so that the company's creditors have no claim to the cryptocurrencies held by the company, particularly in the event of insolvency.

IX. Prevention of the use of clients' crypto assets for own account

ILIRIKA does not use the crypto assets of clients held in the collective account for its own purposes under any circumstances.

The company acts exclusively in accordance with the instructions of its clients in all matters relating to their crypto assets, which means that ILIRIKA cannot generate any income directly from the crypto assets of its clients, except by paying the appropriate fees for the services provided by ILIRIKA[1] .

X. Contingency and recovery plans

The custodian has contingency and recovery plans in place for the custody service. At the same time, there is a contingency plan for restoring the internal reservation system (Shark application), through which client portfolios can be clearly assigned to clients. The plans are reviewed regularly to ensure they are up to date and adjusted as necessary.

XI. Transparency requirements

The custodian must report to its clients at least every three months and at their request on the current positions of their crypto asset holdings held in custody by the custodian. The custodian provides these reports to its clients free of charge.

The company is not obliged to participate in distributed ledger technology (DLT) events that create new rights for the client. An example of such an event is a "hard fork", in which the relevant blockchain is split into one or more parts and new cryptographic values are created. Another example is "airdrops", which can result in the allocation of new crypto assets to a crypto asset wallet. In this case, allocation to individual client accounts is not possible.

XII. Information on risks associated with custody services

The purpose of this section is to inform customers about the main risks associated with crypto asset custody. This list is not exhaustive and does not cover all possible risks that may arise due to technological, regulatory or market changes. We therefore advise clients to familiarise themselves thoroughly with the potential risks and, if necessary, seek independent legal and financial advice.

i. Market risk

The value of crypto assets fluctuates significantly and may lose considerable value in a short period of time. The custodian accepts no responsibility for any loss or increase in their value.

ii. Technological risk

Technical problems such as software bugs, network failures or vulnerabilities in blockchain protocols may result in losses or limited access to crypto assets.

[1] Based on regulatory obligations, several scenarios require actions to be taken in relation to client funds without their instructions; these include blocking or freezing accounts, complying with orders from supervisory authorities or regulatory measures, etc. .

iii. Security risk

Crypto assets may be subject to cyber attacks, including hacker attacks, phishing or malware. Even if the custodian takes security measures, there is a risk that customer assets will be lost due to unauthorised access.

iv. Custodian risk

In the case of third-party storage, there is a risk that the provider may not fully comply with the security standards of the crypto asset custodian, which may result in losses or limited access.

v. Key management risk

Secure management of private keys is essential for accessing crypto asset holdings. Loss or theft of a private key can result in the complete loss of stored crypto assets.

vi. Legal risk

Crypto assets and their storage are regulated differently across the EU and globally. Changes in legislation or legal requirements may restrict storage or impose additional obligations.

vii. Transaction risk

Transactions are usually irreversible. Incorrect entries of destination addresses or transaction details may result in the irreversible loss of crypto assets.

viii. Time delays

Due to variable network utilisation and dependence on blockchain confirmations, delays in transaction processing may occur, affecting access to or use of crypto assets.

ix. Commission risk

High network costs or unexpectedly rising transaction fees may reduce the efficiency and profitability of transfers.

10. Liquidity risk

In the event of high demand or limited liquidity, delays or unfavourable transaction conditions may occur.

XIII. Storage risks and measures to mitigate them

a. Operational risk

The operational risk associated with the custody of clients' crypto assets is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, including legal and regulatory risks.

i. External theft and fraud

External theft and fraud include theft or fraudulent acts by external parties for financial or personal gain.

ILIRIKA addresses risks such as theft, social engineering, phishing and system security breaches through comprehensive monitoring and surveillance. Monitoring includes strict account verification procedures, continuous transaction monitoring and tracking of cryptocurrency transactions for suspicious activity. ILIRIKA also monitors cases of suspected fraud and implements preventive measures to ensure the security and protection of client funds. In addition, ongoing risk assessments and security measures are implemented to protect against cyber attacks and internal threats.

ii. Internal fraud

Internal fraud such as intentional theft or misappropriation of clients' cryptographic assets. All employees of the company are responsible for identifying and reporting suspected cases of internal fraud or potential vulnerabilities.

The company mitigates the risks of internal fraud through a combination of measures, including a rigorous hiring process that ensures ethical and competent employees, including background checks, a clear policy and procedure for reporting internal fraud and whistleblowing, a risk identification and assessment procedure to detect internal fraud risks, coordination procedures, and four-eyes reviews to ensure that the relevant risks are prevented and mitigated.

iii. Process management vulnerabilities

Vulnerabilities in process execution and management include risks related to inaccurate or untimely execution of processes, which may be the result of human error or inefficient processes.

The company uses several control mechanisms to address these risks, including multiple approvers and thorough documentation of internal transfers.

iv. Custodian partner management

Custodian partner management risks include potential threats and vulnerabilities arising from ILIRIKA's cooperation with custodian partners. These risks include, for example, service disruptions, operational problems and financial instability of service providers.

To mitigate these risks, the company implements several control mechanisms, including thorough due diligence and risk assessments at the outset and on an ongoing basis, transparent cooperation agreements containing detailed service level agreements (SLAs) , continuous monitoring of custodial partners and performance reviews, and incident response plans.

b. Information and communication technology (ICT) risks

Information and communication technology (ICT) risk refers to potential business disruptions caused, among other things, by unauthorised access from external threats or internal staff, technical deficiencies and inadequate security practices of custodial service providers. Other risks include system unavailability, weak incident detection and response, and insufficient security awareness leading to phishing attacks.

To manage these risks, the company has implemented a comprehensive information security framework in line with best practices. Controls include role-based access with regular reviews, multi-layered restrictions on access to key material, and advanced security measures such as multi-signature wallets or multi-party computation technology used by the sub-custodian. Regular audits of custodial partners, system monitoring and fault reporting are in place, as well as firewalls, network segmentation, anti-malware tools, vulnerability scanning and external penetration testing. In addition, the company conducts annual awareness training and regular internal phishing tests, and has established a crisis management process to deal with potential incidents.

XIV. Responsibility of the custodian

a. Contractual and legal limitation of liability

ILIRIKA is liable to its customers for the loss of crypto assets or means of access to crypto assets due to an incident attributable to it. ILIRIKA's liability in relation to crypto assets is limited to the market value of the lost crypto assets at the time of loss.

The company is liable without limitation for intent and gross negligence and for any culpable injury to life, limb or health.

In the event of data loss, the company's liability is limited to the costs that would have been incurred even if the customer had made appropriate backups of the data for its recovery. This limitation does not apply to violations of the General Data Protection Regulation (GDPR).

The limitation of liability also applies accordingly to the employees, representatives and vicarious agents of the controller.

b. Scope of insurance coverage

The company indirectly benefits from the sub-controller's insurance policies.

c. Insurance claims procedure

The company ensures the efficient coordination, submission and settlement of claims and maintains transparent communication with customers throughout the process.

XV. Forks and air bubbles

The Company defines two possible scenarios in accordance with Article 75(4) of MiCA, namely:
1. basic software protocols related to any crypto asset available at the company, in relation to which sudden changes in operating rules (hereinafter: forks) may occur;
2. distribution of crypto assets ("airdrops").

The Company has no control over the software protocols governing crypto assets. Support for forks or airdrops depends on several factors:

- technical feasibility: the ability of the custodian's infrastructure to adapt to the changes brought about by forks or airdrops;
- Security considerations: Support must not compromise the security of the infrastructure or customer assets;
- Market impact: Potential effect on the value and functionality of crypto assets;
- Custodian policies: In the event of the scenarios described above, the custodian's position must be taken into account.

The company shall make reasonable efforts to notify customers of upcoming forks or airdrops via its website. The notifications will indicate the Company's support status, and customers should review them in order to make informed decisions about their crypto assets, including any instructions for withdrawal.

XVI. Returning crypto assets to customers

The company has established procedures to ensure the return of crypto assets to customers:
– Transaction monitoring and reporting: To ensure accuracy and legitimacy, the company continuously monitors activity on the client's crypto asset account.
– The company's business continuity plan ensures continuity and security during disruptions.

The company does not allow clients to transfer crypto assets from their crypto asset accounts to external wallets or from external wallets to their crypto asset accounts. A client may only deposit funds from their previously identified transaction account into their crypto asset account or dispose of their crypto assets and transfer the funds received to their previously identified transaction account.

XVII. Reducing the risk of loss of crypto assets

To reduce the potential risks associated with the custody and management of crypto assets, the sub-custodian has established a comprehensive operational framework. This framework includes various documents, procedures and protocols designed to mitigate threats and protect crypto assets from loss. Key principles of wallet and key management include segregation of duties, restricted staff access, multiple transaction approvers, physical security and logical access security. Security measures for accessing the sub-custodian's platform are also a key component. In addition, the framework includes a well-defined process for approving the movement of crypto assets and thorough documentation of internal processes and procedures. Strict general system controls are in place,

covering account verification, fraud monitoring, system security, transaction monitoring and ensuring high availability and business continuity.

XVIII. Sub-custodian oversight and monitoring

A comprehensive and structured approach is used to ensure the control and management of sub-custodian authorisations. This approach is designed to maintain the integrity, security and compliance of all delegated functions. The following sections describe the parameters and processes involved in supervising relationships with sub-custodians and their operations:

a. Regulatory status

The Company only works with sub-custodians that are licensed to provide services under MiCA.

b. Reliable sub-custodian selection process

The company selects sub-custodians after careful consideration of qualitative and quantitative indicators.

c. Strict monitoring process

The company carefully monitors the operations and performance of the sub-custodian.

d. Service Level Agreement (SLA)

The SLA contains detailed provisions on the level of service.

e. Annual due diligence review

The company conducts an annual due diligence review of the sub-custodian.

f. External contractor assessment and exit strategy

In accordance with the Outsourcing Policy, an assessment of the external contractor and an exit strategy are prepared.

XIX. Legal succession of the balance on the client's crypto asset account

In the event of the client's death, the crypto assets in the client's crypto asset account are transferred to the deceased client's heirs, and the custodian continues the contractual relationship with the heirs of that client. If there are several heirs, the heirs must appoint a joint representative in relation to the custodian, who will exercise the rights under the custody agreement concluded with the deceased client.

XX. No deposit protection for crypto assets

Crypto assets held by ILIRIKA for its clients are not subject to deposit protection, as they are not covered by the statutory deposit protection scheme for Slovenian banks (https://www.bsi.si/financna-stabilnost/jamstvo-za-vloge-v-bankah.