Hoppacard d.o.o.

AML / CTF Policy

Company name:
Address:
National Registration Number:
Tax ID:

DOCUMENT INFORMATION	
Policy Owner	Chief Compliance Officer
Purpose	To set out how the firm will mitigate the risk of Money Laundering and Terrorism Finance
Audience	All
Business Unit	Compliance
Approval date	March 2025
Review date	October 2025
Approving Body	Risk and Compliance Committee
Final Approving Body	Board

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS	
Related Policies	Fraud Policy, ABC Policy

APPROVAL INFORMATION			
Document Drafted By	Aleksandar Karać	MLRO	02/10/2025
Document Approved By	Igor Lavrih	Senior Executive Officer/CEO	02/10/2025
Document Updated By	Igor Lavrih	Senior Executive Officer/CEO	02/10/2025
Document Approved By	Igor Lavrih	Senior Executive Officer/CEO	02/10/2025

VERSION CONTROL		
VERSION	**DATE APPROVED**	**KEY CHANGES**
1.0	22/03/2024	Formulation
1.1	22/03/2025	Cleanup
1.2	02/10/2025	Update and reformulation

1 INTRODUCTION & PURPOSE

This Policy establishes and maintains systems and controls to prevent opportunities for money laundering and to ensure that the Board and senior management of Hoppacard d.o.o. (the "Company") remain aware of the effectiveness of our AML controls. This AML Policy therefore helps us in complying with applicable AML & CFT legislation and formalises our arrangement for the annual risk assessment of our AML & CFT program.

The standards set out in this policy are minimum requirements based on applicable legal and regulatory requirements, and these are intended to prevent Hoppacard d.o.o., our employees and clients from being misused for money laundering, terrorist financing or other financial crime.

Responsibility for compliance with this policy lies with each of us and therefore we must always be vigilant and mindful in performing our duties in relation to this policy. The Company has a zero tolerance for money laundering and terrorist financing and is committed to detecting, deterring, countering and mitigating the risks of the Company being used to facilitate money laundering and/or terrorist financing. The Company will take the necessary preventative actions and will promptly investigate any suspicion of money laundering or terrorist financing occurring.

For the purpose of this policy, references to money laundering also include any activities relating to terrorist financing.

This policy will be communicated to all staff during their induction to the Company and any updates will be communicated via email from the MLRO.

Hoppacard d.o.o. is not licensed as a Payment Institution or a Virtual Asset Service Provider and does not fall under direct financial supervisory obligations in these categories. However, it voluntarily adopts and maintains AML/CTF measures aligned with applicable EU standards and national regulations where relevant.

DEFINITIONS

The phrases used in this Procedure shall mean:

1. **AML Analyst** - An Employee or board member of Hoppacard d.o.o., responsible for ensuring that the activities of Hoppacard d.o.o. and its Employees and other persons performing activities for Hoppacard d.o.o. follow anti-money laundering and counter-terrorist financing regulations. The AML Analyst is also responsible for, among other things, submitting on behalf of Hoppacard d.o.o. the notifications referred to in sections XII - XVI of the Procedure.
2. **Hoppacard d.o.o.** - Hoppacard d.o.o. with its registered office in Slovenia.
3. **Beneficial Owner** - any natural person who directly or indirectly controls the Client through the powers he or she possesses as a result of legal or factual circumstances, enabling him or her to exercise decisive influence on the actions or activities undertaken by the Client, or any natural person on whose behalf a business relationship is established, or an occasional transaction is carried out, including:
   a. **in the case of a legal entity other than a company whose securities are admitted to trading on a regulated market that is subject to disclosure requirements under European Union law or equivalent third-country law:**
      i. a natural person who is a shareholder holding more than 25% of the total number of shares in that legal person,
      ii. a natural person holding more than 25% of the total voting rights in the governing body of a legal person, also as a pledgee or usufructuary or under agreements with other holders entitled to vote,
      iii. a natural person controlling the legal person or legal persons, who together hold more than 25% of the total number of shares in that legal person, or who together hold more than 25% of the total number of votes in the governing body of that legal person, including as a pledgee or usufructuary or under agreements with other holders entitled to vote,
      iv. a natural person controlling a legal person through holding powers referred to in Art. 3.1.37 of the Accounting Act of 29 September 1994 (Journal of Laws of 2021, item 217), or
      v. a natural person in a senior position where there is documented impossibility to establish, or doubt as to the identity of the natural persons referred to in the first, second, third and fourth indents, and where there is no suspicion of money laundering or terrorist financing;
   b. in the case of a trust:
      i. founder (settlor), including the founder within the meaning of the Family Foundations Act of January 26, 2023,
      ii. trustee, including the member of the management board within the meaning of the Family Foundations Act of January 26, 2023,
      iii. a supervisor, if any, including the member of the supervisory board within the meaning of the Family Foundations Act of January 26, 2023,
      iv. the beneficiary, including the beneficiary within the meaning of the Family Foundations Act of January 26, 2023, and/or, where the natural persons benefiting from the given trust have not yet been identified, the group of persons in whose main interest the trust was created or operates,
      v. other natural person exercising control over the trust or family foundation,

vi. other natural person having powers or performing duties equivalent to those referred to in indents i. to v. above;

c. in the case of a natural person acting in the course of his business activity, in respect of whom no indication or circumstances have been found that may indicate control by another natural person or persons, such natural person shall be assumed to be the beneficial owner at the same time.

4. **PEP Family Members -** it is understood:
   a. a spouse or a person cohabiting with a politically exposed person;
   b. a child of the politically exposed person and his spouse or cohabitant;
   c. parents of a politically exposed person.
5. **Directive 2015/849** - Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
6. **Terrorist Financing** - means the act defined in Article 165a of the Act of 6 June 1997. - Penal Code.
7. **GIIF** - General Inspector of Financial Information.
8. **Client** - a natural person, legal person or organisational unit without legal personality, who intends to conclude or has concluded an agreement with Hoppacard d.o.o. concerning the provision of services in the scope:
   a. exchanges between virtual currencies and means of payment,
   b. exchanges between virtual currencies,
   c.
   d.
9. **Monitoring** - observation of business relations with the Client, collection or supplementation of information and documentation on the Client, analysis of the Client's Transactions, inter alia: the scale, frequency, types of operations performed on the Account, directions of cash flow, titles of payments, for possible occurrence of suspicious Transactions.
10. **Member State** - a Member State of the European Union or a Member State of the European Free Trade Association (EFTA) - party to the Contract on the European Economic Area.
11. **Persons known to be close associates of PEP -** these are:
    a. natural persons who are the Beneficial Owner of a legal person, organizational units having no legal personality or trust together with a PEP or having other close business relations with such a person;
    b. natural persons who are the sole Beneficial Owner of a legal person, organizational units having no legal personality or trust known to have been created for the purpose of obtaining an effective benefit for a PEP.
12. **PEP** - (Politically Exposed Person) – a natural person occupying prominent public posts or fulfilling prominent public functions, excluding group of middle-ranking or more junior posts, including:
    a. heads of state, heads of government, ministers, deputy ministers, secretaries of state, including the President of the Republic of Slovenia, the Prime Minister and the Deputy Prime Minister;
    b. members of parliament or similar legislative bodies, including deputies and senators,
    c. members of the governing bodies of political parties;

d. members of supreme courts, constitutional courts and other high-level judicial bodies, whose decisions are not subject to appeal, except in extraordinary procedures;
e. members of courts of auditors or of the boards of directors of central banks;
f. ambassadors, chargés d'affaires and senior officers of the armed forces;
g. members of administrative, management or supervisory bodies of state enterprises, companies with State Treasury shareholding, in which more than half of the shares belong to the State Treasury or other state legal persons;
h. directors, deputy directors and members of the organs of international organisations or persons performing equivalent functions in such organisations;
i. managing directors of supreme and central offices of state authorities and managing directors of voivodeship offices;
j. other persons holding public office or performing public functions in State bodies or central government administration bodies.

The list of public positions and functions that are politically exposed positions in other European Union Member States and at the level of international organizations and European Union institutions and bodies is included in the document "Prominent public functions at national level, at the level of International Organisations and at the level of the European Union Institutions and Bodies" (C/2023/724) of 10/11/2023. The link to the aforementioned document is provided in Annex 3 to the Procedure.

13. **Financial services provider** - an institution which has its registered office outside the territory of the Republic of Slovenia and conducts on its own behalf and for its own account, on the basis of a permit of a competent state supervisory authority over such an entity, specified activities;
14. **Employee** - person employed by Hoppacard d.o.o. on the basis of an employment contract or a civil law contract, including a B2B contract. A Member Management Board of the Hoppacard d.o.o. is also considered an Employee.
15. **Money Laundering (ML**) - an offence referred to in Article 299 of the Criminal Code Act.
16. **Execution of Transactions** - the execution by Hoppacard d.o.o. of an order or instruction of the Client or a person acting on its behalf.
17. **Procedure** - this Internal anti-money laundering and counter-terrorist financing procedure at Hoppacard d.o.o..
18. **Account** - the account referred to in point II.8.d of this Procedure.
19.
20. **Regulation 765/2006 –** Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine.
21. **Regulation 269/2014 –** Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.
22. **Legal Tender -** legal tender issued by the National Bank of Slovenia, foreign central banks or other public administration authorities or electronic money.
23. **Register** - the Central Register of Beneficial Beneficiaries referred to in the Act or the register referred to in Article 30 or Article 31 of Directive 2015/849 kept in the relevant Member State. Central Register of Beneficial Beneficiaries is provided on the website

24. **Regulation 910/2014** - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
25. **Regulation 833/2014** – Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.
26. **Electronic Identification Mean -** an electronic identification mean as referred to in Regulation (EU) No 910/2014.
27. **Transaction** - shall be understood as a legal or factual act on the basis of which the transfer of ownership or possession of property values is carried out, or a legal or factual act carried out in order to transfer ownership or possession of property values. A Transaction should also be understood an Occasional Transaction.
28. **Occasional Transaction** - means a Transaction that is not carried out within the framework of the Contract (business relationship).
29. **Contract** - the contract for the provision of services referred to in point II.7.a – d. of this Procedure, which Hoppacard d.o.o. has concluded with the Client.
    a. legal tender issued by the NBP, foreign central banks or other public administration authorities,
    b. an international unit of account established by an international organisation and accepted by individual countries belonging to or cooperating with that organisation,
    c. electronic money within the meaning of the Act of 19 August 2011 on payment services,
    d. a financial instrument within the meaning of the Act on Trading in Financial Instruments of 29 July 2005,
    e. a bill of exchange, a promissory note or a cheque,

    and it may be exchanged for legal tender and accepted as a medium of exchange in economic transactions and may be stored or transferred electronically or traded electronically.
30. **Property Values** - property rights or other movable or immovable property, means of payment, financial instruments within the meaning of the Act of 29 July 2005 on trading in financial instruments, other securities, foreign exchange values and Virtual Currencies;
31. **Application** - the Client's application to conclude a Contract with Hoppacard d.o.o..
32. **Suspension of Transactions** - a temporary restriction on the ability to use of Property Values by preventing Hoppacard d.o.o. from carrying out a specific Transaction or more specific Transactions.

I. RESPONSIBLE PERSONS AND SUPERVISION

1. Designated Member of Management Board of the Hoppacard d.o.o. overseeing anti-money laundering and counter-terrorist financing area:
    a. is responsible for the implementation and performance by Hoppacard d.o.o. of the obligations set out in the Act;
    b. supervises the implementation of obligations under the Act;
    c. accepts, after obtaining the opinion of the AML Analyst, Clients: PEP, Persons known to be close associates of PEP, PEP Family Members and Clients associated with a high-risk third country as identified in Annex 1 to the Procedure;
    d. approves Hoppacard d.o.o.'s action projects necessary for the proper implementation of Hoppacard d.o.o. obligations under the Act;

e. prepare at least once a year a report on the performance of its own tasks, which it shall submit to the Management Board (if the Management Board consists of more than one person) and the Supervisory Board, by the end of the first quarter following the year to which the report relates;

f. ensure that the AML Analyst prepares and submits the report referred to in point III.2.q of the Procedure;

g. informs the Management Board (if the Management Board consists of more than one person) at once of any serious or significant anti-money laundering or/and counter-terrorist financing incidents and violations and of the recommended corrective actions;

h. ensures that the AML Analyst has direct access to all information necessary to perform his/her tasks, has sufficient human and technical resources and tools to adequately perform his/her tasks, is well informed of incidents and Hoppacard d.o.o. misconducts;

i. ensures that the AML Analyst is able to contact him (Designated Member of Management Board) directly;

j. considers and, where appropriate, takes appropriate action on comments made to him by the AML Analyst on relevant anti-money laundering and/or counter-terrorist financing issues at Hoppacard d.o.o..

2. AML Analyst:

a. ensures compliance of the activities of Hoppacard d.o.o. and its employees and other persons performing activities on behalf of Hoppacard d.o.o. with the legal provisions on anti-money laundering and counter-terrorist financing;

b. review and sign all correspondence sent to supervisory authorities, in particular notifications of suspicious transactions and circumstances that may indicate the suspicion of money laundering or terrorist financing;

c. draw up periodic reports in the area of Anti-Money Laundering and Terrorist Financing and submit them for approval to the Hoppacard d.o.o. Management Board;

d. give its opinion on training programmes and carry out the training of Employees;

e. analyses Transactions and monitors business relations with Clients;

f. typifies circumstances that may indicate a suspicion of Money Laundering or Terrorist Financing offences or Transactions that should be reported to the GIIF or the Prosecutor's Office;

g. draw up the information and notifications to the authorities, in particular those referred to in points XII to XVI of the Procedure;

h. reviews and signs all correspondence addressed to the supervisory authorities, including in particular notifications of Transactions (in accordance with the power of attorney to make such declarations granted by Hoppacard d.o.o.);

i. prepares replies to letters/inquiries received from the GIIF or the Prosecutor's Office and other authorities;

j. accepts Clients: PEP, persons known to be close associates of PEP, family members of PEP and Clients affiliated with a high-risk third country indicated in Annex 1 to the Procedure (if such authority is granted to it by the Hoppacard d.o.o. Management Board) and other high-risk Clients;

k. cooperates with Hoppacard d.o.o. anti-money laundering staff;

l. prepare and deliver anti-money laundering or counter-terrorist financing training programmes;

m. coordinates the implementation of the mandatory AML and CFT training by Employees;

n. reviews Hoppacard d.o.o. products, services and internal regulations for compliance with generally applicable anti-money laundering and counter-terrorist financing legislation;

o. verifies the correctness and supervises the completeness of the data collected by the Employees for the identification, verification and acceptance of the Client;

p. shall be responsible for the Suspension of Transactions, freezing of the Property Values, non-provision of the Property Values and execution of orders and demands of competent authorities, in particular GIIF and prosecutor's office

q. prepare at least once a year a report on the performance of its own tasks, which it shall submit to the Management Board and the Supervisory Board by the end of the first quarter following the year to which the report relates;

r. be immediately available for a meeting with the GIIF, a public prosecutor or other law enforcement authority;

s. reports on any material incident to the Supervisory Board and the Management Board;

t. recommends to the Management Board the corrective measures to be taken in Hoppacard d.o.o. in order to eliminate the identified misconduct in the performance of anti-money laundering and/or counter-terrorist financing obligations;

u. report the need for human or technical resources or the need to implement new measures or solutions to the designated Member of Management Board of the Hoppacard d.o.o. overseeing anti-money laundering and counter-terrorist financing area;

v. regularly reviews the reasons why warnings of unusual activity or Transactions have not been communicated to him/her to determine whether there are issues that need to be addressed to ensure effective detection of suspicious activity or Transactions.

3. Supervisory Board of Hoppacard d.o.o.:

   a. shall review the performance reports received from the AML Analyst and designated Member of Management Board of the Hoppacard d.o.o. overseeing anti-money laundering and counter-terrorist financing area;

   b. may request any information, reports, audits, results of audits, correspondence with government authorities and other data held by Hoppacard d.o.o. and relating to the performance of its anti-money laundering and counter-terrorist financing obligations;

   c. shall evaluate at least once a year the effectiveness of Hoppacard d.o.o.'s performance in complying with its anti-money laundering and counter-terrorist financing obligations.

4. Management Board of Hoppacard d.o.o. shall:

   a. review and, where appropriate, respond to the performance reports received from the AML Analyst;

   b. ensure that the Supervisory Board has access to all information, reports, statements, audit results, correspondence with governmental authorities and other data held by Hoppacard d.o.o. and relating to the performance of its anti-money laundering and counter-terrorist financing obligations;

   c. consider and respond to information received about incidents or misconduct at Hoppacard d.o.o..

II. GENERAL PROVISIONS

1. Hoppacard d.o.o. does not handle client funds — whether fiat currency or virtual assets — directly. All such activities, including the custody, exchange, settlement, and transmission of funds, are executed by regulated third-party service providers with appropriate licensing and compliance frameworks. Hoppacard d.o.o. does not operate as a VASP, PSP, or custodian and therefore does not fall under direct supervision for such activities, but maintains robust AML/CTF oversight and third-party risk management for any partners engaged in such functions.
2. Hoppacard d.o.o. maintains a third-party risk management framework to assess and monitor the AML/CTF compliance of all external service providers involved in processing, custody, or transmission of value on behalf of the Company or its clients. This includes due diligence at onboarding, review of licensing status, publicly available enforcement history, and periodic reassessment of their compliance practices.
3. Hoppacard d.o.o. employees who conduct Client's service must establish the true and current details of Clients intending to enter into a Contract (establish a relationship) with Hoppacard d.o.o. and of Clients already using Hoppacard d.o.o. services and products.
4. Hoppacard d.o.o. employees, in the event that it is found that information about a Client, in particular its Transactions, is not consistent with Hoppacard d.o.o.'s knowledge of the Client in question, its business profile, risks and sources of funds, are obliged to report such transactions to the AML Analyst.
5. Hoppacard d.o.o. does not offer products or services that allow to remain anonymous by Client.
6. The provisions of the Procedure relating to the Supervisory Board shall only apply if there is a Supervisory Board in Hoppacard d.o.o..
7. Each Hoppacard d.o.o. Employee shall promptly make available to the AML Analyst any information and documents that the AML Analyst requests for the purpose of performing his/her duties under the Procedure. The decision as to what information and documents the AML Analyst must have access to rests solely with the AML Analyst.

2 REVIEWS OF POLICY

This policy will be reviewed on at least an annual basis with ad hoc and periodic updates done as considered necessary by the Company's Management Body in the event of changing circumstances, laws, rules, guidelines and regulations.

3 RESPONSIBILITIES

Responsibility for compliance with this policy lies with all employees of the Company, however all AML related matters, concerns and queries including operations surrounding AML/CFT lies with the Money Laundering Reporting Officer ('MLRO') The MLRO is also vested with the authority and responsibility to implement the policies, procedures and controls set forth herein.

All employees are responsible for reporting AML/CTF concerns internally, including any issues arising from the conduct or regulatory status of third-party providers. Such concerns must be reported to the MLRO without delay.

The Company's MLRO is Aleksandar Karać. Please reach out to the MLRO with any questions about this policy or money laundering concerns.

4 REGULATORY FRAMEWORKS

This AML Policy is designed to include guidance on compliance with the laws of European Union("EU), Act 1 of 1 March 2018 on counteracting money laundering and financing of terrorism, Polish Financial Supervision Authority (PFSA) and other relevant international AML & CFT and sanctions laws, rules and regulations.

4.1 APPLICABLE LAWS & REGULATIONS

There are several AML & CFT laws, rules and regulations that apply to Hoppacard d.o.o.. The key laws and regulations are mentioned below:

- Directive (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Directive (EU) 2015/849 of the European Union
- Directive (EU) 2015/2366 of the European Union
- Act 1 of 1 March 2018 on counteracting money laundering and financing of terrorism
- Any other Federal legislation relating to money laundering, terrorist financing, the financing of unlawful organizations or sanctions non-compliance.
- See "Definitions" for other Acts and Directives

Under these laws an employee and/or Hoppacard d.o.o. may be criminally liable for the offence of money laundering if such an activity is intentionally committed in its name or for its account. Hoppacard d.o.o. and you may also be liable for breach of the PFSA rules and potentially breaking the laws, if you fail to abide by this policy and other related procedures that are aimed at preventing money laundering and other types of financial crime. You must also keep in mind that failure to report suspicions of money laundering, "tipping off" or assisting in the commission of money laundering may each constitute a criminal offence that is punishable under the laws of Slovenia and the European Union.

5 Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income. The risks to the financial sector primarily involve being used to facilitate this process, whether knowingly or unwittingly.

Terrorist Financing is all dealings with funds or property which are, or are likely to be, used for the purposes of terrorism, even if the funds are "clean" in origin.

5.1 Stages of Money Laundering

Money laundering is generally broken down into in three distinct stages:

- Placement Stage
- Layering Stage
- Integration Stage

A. The Placement Stage

The placement stage represents the initial entry of the "dirty" cash or proceeds of crime into the financial system. Generally, this stage serves two purposes: it relieves the criminal of holding and guarding large amounts of bulky of cash and it places the money into the legitimate financial system.

B. The Layering Stage

After placement comes the layering stage (sometimes referred to as structuring). The layering stage is the most complex and often involves the international movement of the funds. The primary purpose of this stage is to separate the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscure the audit trail and sever the link with the original crime.

C. The Integration Stage

The final stage of the money laundering process is termed the integration stage. It is at the integration stage where the money is returned to the criminal from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

- Non-face to face nature of interactions making it more difficult to verify who the client is therefore heightening the Money Laundering risk.

5.2 Money Laundering and Terrorist Financing Offences

5.2.1 Key money laundering offences

A money laundering offence may be committed if a person/entity:

- Conceals, disguises, or transfers criminal property.
- Enters into or becomes involved in an arrangement which he knows, or suspects facilitates the acquisition, retention, use or control of criminal property on behalf of another person; or ● Acquires, uses, or has possession of criminal property.

An entity may also be criminally liable and punishable under the laws of the Slovenia and European Union for the offence of money laundering if such activities are intentionally committed in its name or for its account, fails to report suspicions of money laundering, tipping off and assisting in the commission of money laundering

The primary money laundering offences each turn on the definition of "**criminal property**". Property is criminal property if it constitutes any benefit from criminal conduct, or it represents such a benefit (in whole or in part, whether directly or indirectly). Criminal property includes money, goods and chattels with a value. Criminal property will also include any gains or profits gained from the original offence, including indirect benefits. If a person obtains a pecuniary advantage as a result of or in connection with conduct, they are to be taken to obtain a sum of money equal to the value of the pecuniary advantage. In short, any criminal conduct that results in a measurable financial benefit is a predicate offence for money laundering purposes. A benefit includes a saving resulting from criminal conduct. There is no de minimis level.

5.2.2 KEY TERRORIST FINANCING OFFENCES

The terrorist financing offences are similar to that set out above for money laundering. Such activities include where the employees of the Company and/or the Company itself:

- are aware that the proceeds/funds are wholly or partly owned by a terrorist organisation or persons;
- are aware that the proceeds/funds are wholly or partly intended to finance a terrorist organisation, a terrorist person or a terrorism crime, even if it's without the intention to conceal or disguise their illicit origin;
- are providing, collecting, preparing or obtaining Proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or if he has committed such acts on behalf of a terrorist organisation or a terrorist person while aware of their true background or purpose.

5.3 CONSEQUENCES OF NON-COMPLIANCE AND PENALTIES

Non-compliance with the money laundering obligations by employees is considered a serious offence and disciplinary action may be taken by the Company, including immediate dismissal. Not only will the persons/entity be subject to regulatory penalties and fines, but it could also cause significant damage(s) to the reputation of the Company and its employees. Failure to comply by an employee may also expose the Company to penalties, censure and enforcement action (including the imposition of fines) by the PFSA or other regulatory bodies.

Failure to comply with the money laundering and terrorist financing obligations and provisions of the relevant laws, rules and guidelines may also result in criminal penalties as prescribed by the relevant supervisory authorities:

a. Persons/entities found guilty of the offence of money laundering shall be subject to imprisonment for a period of three months to Five years.

b. Persons/entities found guilty of the offence of terrorist financing shall be subject to imprisonment for a period of three months to Five years

Person/entities involved in the act of 'tipping off' will also be subject to Imprisonment of three months to five years. Where the person has acted unintentionally, they will be subjected to a fine.

6 Risk management and Controls

6.1. Applying a Risk-Based Approach ('RBA")

To ensure that we appropriately address the AML and CFT risks originating from our business, we have adopted a risk-based approach. This approach takes into consideration our business, type of clients, their domicile, and the way we engage with them. The senior management of the Company commits to:

- establishing clear standards for accepting clients which may involve further Enhanced Due Diligence (EDD) as the risk of the client increases;
- establishing procedures relating to client identification and screening against databases to access acceptability;
- procedures relating to client profiling which help identify the reason our clients establish a business relationship with the Company;
- providing clear guidance when and under what conditions reliance can be placed on the AML/Know Your Customer (KYC) profiling or screening performed by affiliated entities or external third parties;
- establishing controlled procedures should a decision arise as to the exit of a client relationship as a result of AML/KYC procedures; and
- appointing a Money Laundering Reporting Officer (MLRO) who would be responsible for the oversight of AML/KYC activities within and on behalf of the Company.

The RBA consists of two elements which are highlighted below.

6.1.1. Business AML Risks

The first step in assessing the AML and CFT risks is for us to take a holistic view of our business. We form this view by assessing the nature, size, and complexity of our activities. The Company has created a risk-based model which covers the following parameters:

- types of clients and their activities;
- countries or geographic areas in which we do business;
- products, services and activity profiles;
- distribution channels and business partners;
- complexity and volume of transactions;
- new products, business practices, delivery mechanisms, channels and partners; and
- the use of new or IT technologies for both new and pre-existing products and services.

The Company also takes appropriate measures to ensure that any risks identified in the assessment are considered in day-to-day operations and are mitigated when taking on new clients; when developing new products, services, business practices and technologies, or when changes occur in our business profile.

In addition to the above risk model, the MLRO conducts a subjective review of the AML risks facing the Company and documents the results in the final risk assessment produced for the Board's review and approval.

Furthermore, the information we obtain through the business risk assessment is used to develop and maintain this policy and all related procedures. The business risk assessment ensures that our AML & CFT controls adequately mitigate the risks identified as part of the annual assessment. It also gives us a framework to assess the effectiveness of our AML & CFT program and assists in the prioritization and allocation of our resources.

When assessing AML/CFT risk, Hoppacard d.o.o. takes into account the risk profiles of its third-party providers involved in the custody, exchange, or movement of value, and ensures that appropriate due diligence is conducted on their licensing and regulatory compliance.

6.1.2. CLIENT RISK

We obtain Know Your Client ("KYC") documents and perform Client Due Diligence ("CDD") for all new clients.

The MLRO also performs an annual review of the CDD process and documentation on file and this annual assessment forms part of the larger review exercise conducted to produce the Annual AML Return and AML Report required by the PFSA.

To ensure that we take on clients in line with our risk profile, we conduct a risk-based assessment on each client. The outcome of this process produces a risk rating for the client, which determines the level of CDD we will apply to that client.

We will not establish a business relationship with any client where the client's ownership or control arrangements prevent us from identifying one or more of the client's beneficial owners.

7 CUSTOMER DUE DILIGENCE

The fundamental basis of effective AML & CTF controls is complete, accurate and up to date client due diligence ("CDD"). Properly completed CDD is important for two reasons:

- The Company is required to check that its clients (and, where relevant, beneficial owners of its clients) are who they say they are and that the transactions and activities carried on with or for each client are consistent with the Company's expectations. Failure to do so means breaching the Company's regulatory obligations.

- Additionally, complete CDD enables the Company to establish what might constitute typical activity as between the Company and that client. This is because it is necessary, once an on-going business relationship has been established, to monitor and review any regular business undertaken for that client against the expected pattern of activity of the client. As part of the Company's commitment to conduct on-going monitoring of circumstances which could give rise to financial crime concerns, any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.

As a result, the Company's CDD broadly consists of:

- Identifying the customer and verifying the customer's identity using documents or information from a reliable and independent source.

- Identifying the beneficial owner(s) and verifying that person's identity, taking measures to understand the ownership and control structure of the customer, where applicable.

- Assessing the purpose and intended nature of the business relationship (business profile).

- Conducting ongoing monitoring of the business relationship and transactions undertaken to ensure that they are consistent with the Company's knowledge of the customer, business, risk profile and source of funds.

The Company will apply CDD measures:

- before it establishes a "business relationship" (as defined below); before it carries out an "occasional transaction" (as defined below);

- if the Company suspects money laundering or terrorist financing;

- if the Company doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification;

- at other appropriate times to existing clients on a risk sensitive basis; and

- when the Company becomes aware that the circumstances of an existing client, which are relevant for its risk assessment of that client, have changed.

A "business relationship" is a business, professional or commercial relationship between the Company and a client, which is connected to the business of the Company, and which is expected by the Company, when the contact is established, to have an element of duration, this includes advice as well as transactions.

An "occasional transaction" is defined as meaning a transaction (carried out other than as part of a business relationship – see above) for amounts equal to or exceeding an amount of equal to or more than Euros 15,000;, whether the transaction is carried out in a single transaction or in several transactions that

appear to be linked; and/or in the form of Bank Transfers for amounts equal to or exceeding Euros 15000. Given the nature of the Company's business and operations, the recommended threshold is EUR 1,000.

The Company will also ensure that anyone acting on behalf of the customer is authorised to do so and will identify and verify the identity of that person.

The Company will ensure that customers are identified and that their identity is verified before commencing any transactions with them.

Given the specific nature of the services provided and assets transacted, Hoppacard d.o.o. deploys a range of onboarding and transaction monitoring tools to identify, mitigate and prevent financial crime:

- [Automated customer risk assessments]

The level of CDD to be undertaken (both initially and for the duration of the business relationship) is determined by reference to the client's risk rating assigned under the Client Risk Assessment.

Beneficial Ownership means a natural person who ultimately owns or controls the client, or a natural person on whose behalf a transaction is conducted, or a business relationship is established.

There are two levels of CDD: Standard/Simplified (for low and medium risk clients) and Enhanced (for high-risk clients).

In cases where customer onboarding or financial transactions involve a third-party provider, Hoppacard d.o.o. relies on the KYC/AML measures conducted by that provider, ensuring that such reliance is based on written agreements and that the provider is appropriately regulated in its jurisdiction.

7.1. TIMING OF CDD

For all new clients, CDD must be gathered by or prior to the time at which any business relationship is formalized, e.g. by the signing of a client agreement or the acceptance of the terms of business.

Exceptionally, subject to the MLRO and the Board's approval, CDD may be completed after this time if:

- deferral is necessary for a time-critical transaction that, if not executed immediately, would or may cause a financial loss to the client due to a price movement or loss of opportunity;
- there is little money laundering risk, or any identified risk is effectively managed; and
- the CDD is completed within 30 days from entering the business relationship.

Where the CDD is not completed within 30 days, the Company must, prior to the end of the 30-day period, document the reason for its non-compliance and complete the CDD as soon as possible.

7.2. ONGOING CLIENT DUE DILIGENCE

We undertake ongoing CDD for all clients. The frequency of this review depends upon the client risk rating, which we conclude through the RBA. This ongoing CDD ensures that the information remains accurate and that we can assess the client's transaction pattern against their business and risk rating. This ongoing process also allows us to ensure that where required, changes to client risk ratings are made at reasonable intervals particularly where the client is moving from low or medium risk to a high-risk category

7.3. CLIENT IDENTIFICATION PROCEDURES

The AML Policy establishes, and the Company will maintain, reasonable procedures designed to verify clients' identities to the extent reasonable and practicable (such procedures are referred to generally as "Client Identification Procedures"). The Client Identification Procedures undertaken with respect to the Company's clients should consider the specific risks presented by each of them.

Client Identification Procedures are based upon the specific characteristics presented by the following types of clients:

- Natural persons
- Corporations, partnerships, and comparable legal entities
- High Risk Clients

7.4. FAILURE TO CONDUCT OR COMPLETE CLIENT DUE DILIGENCE

Where the Company is unable to complete the appropriate and required due diligence checks it will not establish a relationship with the client(s) nor provide any of its products and services to its clients. Consideration will also be taken as to if a Suspicious Activity Report (SAR) is to be made.

7.5. ALLOCATION OF RESPONSIBILITIES BETWEEN THE PARTIES

Agreements with third parties, whether placement agents or administrators, should clearly allocate responsibilities for compliance with applicable AML law and regulation as well as the law and regulations applicable in the fund's home Slovenia jurisdiction between the third-party and the related fund and the Company, as appropriate. Agreements with third parties should also seek to establish effective lines of communication for addressing client due diligence issues and suspicious activity or circumstances as they arise and provide a means by which the Company may periodically verify or audit the third-party's compliance with its AML policies, procedures and controls.

8 ROLES AND RESPONSIBILITIES

Through this policy, we have mandated the Money Laundering Reporting Officer (MLRO) and in their absence the Deputy MLRO (DMLRO):

- to have direct access to the Board;
- to determine the level of resources required to perform his duties in an effective, objective and independent manner;
- to have status of Senior Manager to enable him to act on his own authority; and
- to have unrestricted access to information sufficient to enable him to carry out his responsibilities.

8.1. RESPONSIBILITIES OF THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

The MLRO has the following responsibilities:

- day-to-day operations for our compliance with the relevant AML & CFT rules and regulations;
- executes a thorough and appropriate AML Compliance Risk Assessment for the Company, its products, its customer base, the countries it has business with, its business third-party relations and its delivery channels, and assign a risk rating to each;
- based on the results of the AML Compliance Risk Assessment, adopt appropriate risk management controls and procedures so as to adequate and continuously avoid exposing the Company to any risks related to money laundering, terrorism financing, proliferation, and financing of illicit organizations and entities;
- executes appropriate customer due diligence for all Politically Exposed Person's (PEP's), or PEP-related individuals and suggest their approval to the Compliance Committee of the Board;
- acts as the point of contact to receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions regarding the prevention of money laundering;
- receive suspicious transaction alerts from employees and analyse them to take appropriate actions and decisions to report all suspicious cases such as filing a SAR or Suspicious Transaction Report (STR);
- on-going monitoring of transactions to identify high-risk, unusual and suspicious customers/transactions;
- provide necessary reports to the Board and the Compliance, Risk and Audit Committee on all AML/CFT issues, on a quarterly basis at a minimum;
- acts as the point of contact in relation to an AML & CFT queries originating from Slovenia and European Union authorities and is responsible for promptly responding to such requests;

- reviews the Policies on an annual basis to ensure that they remain up to date not only in relation to the law and regulations but also the recommendations from international bodies such as the FATF and Wolfsburg forum;
- establishing and maintaining appropriate AML policies and procedures;
- ensuring that the Company and its employees meet their fiduciary responsibilities to clients;
- the general administration of the policies and procedures set forth in this Policy;
- review all reports submitted pursuant to this Policy, answer questions regarding the policies and procedures set forth in the Policy, update this Policy as required from time to time, and arrange for appropriate records to be maintained, including copies of all reports submitted under this Policy;
- reviewing at least annually, the adequacy of the policies and procedures of the Company and the effectiveness of their implementation;
- investigate any possible violations of the policies and procedures set forth in this Policy to determine whether sanctions should be imposed, including, *inter alia*, a letter of censure or suspension or termination of employment of the violator, or such other course of action as may be appropriate;
- for the Company's compliance with all laws and regulations, among other duties this covers a responsibility to ensure the filing and updating of all required forms and documents as applicable under the laws and regulations of the various jurisdictions under which the Company operates; and
- reporting to the Board and PFSA on the status of the Company's compliance with relevant AML laws and rules, and for ensuring that all communication with the PFSA is done in an open and cooperative manner, disclosing any information the PFSA would reasonably expect to be notified.
- If employees become aware of any misconduct or regulatory action involving third-party partners, they must promptly escalate this to the MLRO, who will assess potential risks and report as appropriate to management or competent authorities.

Any complaint, whether written or oral, relating to AML & CFT must be brought to the attention of the MLRO immediately. Any response to such client complaints must be in writing and requires the approval of the MLRO. Any inquiry from any member of the press relating to AML & CTF matters must be referred to the MLRO. In the event any federal, state, or self-regulatory organization contacts the Company (either in writing or by telephone) or arrives for an inspection, the MLRO must be promptly notified.

8.2. The Risk, Audit & Compliance Committee (RACC)

The ARCC consists of the SEO, Board of Directors, Risk Officer and the COMLRO. This Committee is responsible for final decisions regarding all matters relating to AML and CFT. They are also notified by the COMLRO of any AML/CFT related activities within the Company.

8.3. MLRO Reporting Requirements

The MLRO will report to the Board on a quarterly and semi-annual basis, regarding the status of AML and CFT compliance. The following reports are to be presented to the Board and the ARCC.

8.3.1. MLRO Semi-Annual AML Report

The MLRO is required to report semi-annually to Board of the Company on:

- the results of any reviews on, and the quality of, the Company's AML Systems;
- the Company's compliance with applicable AML legislation and regulations;
- any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions and how the Company takes them into account;
- any internal Suspicious Activity Reports and the action taken in respect of those reports, including the grounds of all decisions;
- any external Suspicious Activity Reports made by the Company and the action taken in respect of those reports including the grounds of all decisions; and
- any other relevant matters related to money laundering and the Company.

The Board must assess the report, take appropriate action on the findings of the report, and resolve any identified deficiencies, and then make a record of such assessment and actions taken.

8.3.2. Annual AML Return

The MLRO also prepares an annual AML return which is submitted to the PFSA by the 31st of December of each year. This return includes details regarding the status of the AML & CFT program, key issues, policy and procedural updates and the nature and type of clients the Company has taken on in the previous year.

9 Training and Awareness

To maintain an effective AML & CFT program, it is imperative that we all understand this AML Policy and are trained to identify and report suspicious activity. To achieve these goals, the Company provides annual AML trained to all relevant persons as soon as reasonably practical after joining the Company, and not less than annually thereafter.

AML training is mandatory for all employees, including Directors, and will be designed to ensure that it remains up to date with money laundering trends and techniques and that it is appropriately tailored to the Company's different activities, services, Customers and indicates any different levels of money laundering risk and vulnerabilities

Relevant persons include the Partners, operational staff, any employee with client contact or who handles client assets and any other person who might potentially encounter money laundering within the business.

The AML training covers the following topics:

- Slovenia and European Union AML law and PFSA legislation relating to money laundering;
- our policies and procedures;
- understanding the types of activity that may constitute suspicious activity;
- how to make notifications to the MLRO;
- prevailing techniques, methods and trends in money laundering; and
- understanding your role in combating money laundering.

The training will also include the following topics to ensure the employees are aware of:

- the roles and responsibilities of Employees in combating money laundering , including the identity and responsibilities of the Authorised Company's MLRO and his deputy;
- applicable legislation relating to anti-money laundering;
- the potential effect on the Company, its Employees and its Customers of breaches of applicable legislation relating to money laundering;
- the Company's anti-money laundering policies, procedures, systems and controls and any changes to these;
- money laundering risks, trends and techniques;
- the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged that may warrant an internal Suspicious Activity Report (SAR);
- the Company's arrangements regarding the making of an internal Suspicious Activity Report (SAR);
- the use of relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in these procedures; and
- requirements relating to Customer identification and ongoing due diligence and scrutiny of Transactions.

9.1. Employee Files & AML Training Register

The MLRO will be responsible for overseeing that each employee has a training log and that their training log is maintained. The MLRO must also maintain an AML Training Register which will detail all relevant details of AML training for a period of at least 6 years including the dates of any training provided, the nature of the training as well as the recipients of the AML training.

9.2. Cooperation with the Regulators

The Company must ensure that it is open and cooperative in all its dealings with the Regulator; and ensure that any communication is in the English language.

9.3. Employee Disclosures

The Company will not prejudice an Employee who discloses an information regarding money laundering to the Regulator or to any other relevant body (including the Financial Intelligence Unit of Slovenia) involved in the prevention of money laundering.
All relevant details of the Company's AML training must be recorded, including:

- dates when the training was given;
- the nature of the training, and
- the names of the employees who received the training.

These records must be kept for at least six years from the date on which the training was given

10 . Suspicious Activity Reports (SAR)

This AML & CFT Policy requires you to monitor and report suspicious activity or transactions in relation to potential money laundering or terrorist financing.

You are required to promptly notify and provide the MLRO with all relevant details, where you either know, suspect or have reasonable grounds for knowing or suspecting that a person (whether a client or not) is engaged in, or attempting money laundering or terrorist financing.

You must decide whether the MLRO should be notified, and you should not be prevented or dissuaded from doing so where suspicion exists or there are reasonable grounds for knowing or suspecting that a person may be involved in money laundering. The requirement to notify the MLRO includes any suspicious activities even when the business relationship has not been developed.

The failure to report a suspicious transaction under any of these circumstances is a serious breach of your duties and will result in disciplinary action.

10.1. Filing Suspicious Activity Reports

The MLRO starts his investigation within 24 hours of receiving a suspicious transaction notification. The investigation may involve reviewing CDD documents, transaction history, speaking to staff and any other method the MLRO deems relevant to arrive at a conclusion. If the investigation results in a decision to file the SAR with the Slovenia Financial Intelligence Unit, the MLRO will do so.

Where following a notification and after conducting the investigation, the MLRO decides not to file a SAR, the MLRO will document the reasons for such determination.

The Company appoints the MLRO as the only authorized person to decide on whether or not to file a SAR and that his decision is made independently and is not subject to the consent or approval of any other person.

All relevant details of any internal or external SAR must be kept for at least six years from the date the report was made.

10.2. Tipping-Off

Tipping-off is defined as an unauthorized act of disclosing information that may result in the Company, client, or a third-party (other than the FIU or the Regulator), knowing or suspecting that the Company or client is or may be the subject of a suspicious transaction report or an investigation relating to money laundering or terrorism financing; and may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorism financing.

You are reminded that you must not tip-off any person, this means you must not inform any person whether a natural person or a legal entity, that he is being scrutinized for possible involvement in suspicious activity related to money laundering, or that any government agency is investigating his possible involvement in suspicious activity relating to money laundering.

If you reasonably believe that performing CDD will tip-off a client or potential client, you may choose not to pursue that process. If you decide as such, you must promptly notify the MLRO, who will decide whether a SAR should be filed. The records outlining the grounds for the belief that conducting CDD or ongoing monitoring would have tipped off a potential or existing client will be retained in accordance with the applicable records keeping regulations.

11 REVIEW OF AML SYSTEMS

The Company will conduct regular reviews and assessments of the effectiveness and compliance with the Company's AML Systems, and will specifically cover the following:

- sample testing of compliance with the Company's CDD arrangements;
- an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and
- a review of the nature and frequency of the dialogue between the Senior Management and the MLRO.

The reviews will be carried out at least annually and the results will be reported to the Board.

The MLRO, under the supervision of the Board, will conduct the appropriate follow-up to ensure that any deficiencies detected during the review are addressed and rectified.

12 REGULATORY REQUESTS

The Company and its employees shall be open and cooperative in their dealings with the PFSA. The Company will inform the PFSA in writing if, during its activities within it:

- receives a request for information from a regulator or agency responsible for AML, counter-terrorism, sanctions, or bribery regarding enquiries into potential breaches;
- becomes aware or suspects that money-laundering, terrorism financing, a sanctions breach, or an act of bribery has occurred or may occur in or through its business;
- becomes aware or suspects that another person outside of its business is engaged in money-laundering, terrorism financing, a sanctions breach, or an act of bribery unless these the information is legally privileged or in the public domain;
- becomes aware of any money laundering or sanctions matter in relation to the Company which could result in adverse reputational consequences; or
- becomes aware of any significant breach of the PFSA AML rules of Slovenia and European Union legislation.

13. NO RETALIATION POLICY

It is our policy to not prejudice in any way the standing of a staff member, who discloses information regarding money laundering to any relevant regulatory authority, government agency or to any other relevant body involved in the prevention of money laundering.

PART TWO

ANTI-MONEY LAUNDERING RISK ASSESSMENT AND CLIENT

IDENTIFICATION PROCEDURES

1. INTRODUCTION

The Anti Money Laundering ("AML") Risk Assessment and Client Identification Procedures provide details of the steps followed by Hoppacard d.o.o. (herein referred to as "Company", "We" or "Us") to comply with the Anti-Money Laundering & Counter Terrorist Financing laws, rules and regulations of the Slovenia and the European Union and the Polish Financial Services Authority ("PFSA").

To counter the money-laundering risks to our business, the Company's management has adopted a risk based methodology that entails the following components:

- AML Business Risk Assessment;
- AML Risk Assessment for the Client;
- Client Due Diligence (CDD) requirements.

We utilise these components to assess AML risks to our business and to take reasonable steps to eliminate or manage these risks. The results of the Business and Client Risk assessments feed into the CDD requirements applied to each new and existing client relationship.

2. RISK ASSESSMENTS

I. BUSINESS AML RISK ASSESSMENT

A key aspect of the Company's AML risk management is the Business AML Risk Assessment. The MLRO conducts the Business AML Risk Assessment annually (or earlier if there is a significant change in the business that warrants a review) to identify and assess any money laundering risks to which the business is exposed, taking into consideration the nature, size and complexity of its activities and, to the extent relevant, any vulnerabilities relating to:

- its type of customers and their activities;
- the countries or geographic areas in which it does business;
- its products, services and activity profiles;
- its distribution channels and business partners;
- the complexity and volume of its Transactions;
- the development of new products and business practices, including new delivery mechanisms, channels and partners; and
- the use of new or developing technologies for both new and pre-existing products and services.

The results are reviewed and approved by the Board.

The Company must use the information obtained in its periodic business risk assessment to develop and maintain its AML policies, procedures, systems and controls, ensure that they adequately mitigate the

risks that have been identified, assess their effectiveness, and assist in the allocation and prioritisation of AML resources and in carrying out its customer risk assessments.

Prior to launching any new product, service, business practice or using a new or developing technology the Company will:

- Assess and identify the money laundering risk related to the product, service, business practice or technology; and
- Taken appropriate steps to mitigate or eliminate the risks identified above.
- The Company while conducting periodic business risk assessment must consider the outcome of the Slovenia and other National Risk Assessments (NRA).

II. CLIENT RISK ASSESSMENT

This section describes the risk-based assessment that must be undertaken on a client and documents the process through which we produce a risk rating for the client. This risk rating is used to determine the level of CDD that will apply to that client.

CDD in this context refers to the process of identifying a client, verifying identification through documentation, and monitoring the client's business and money laundering risk on an on-going basis.

To undertake a risk-based assessment of every client and to assign the client a risk rating, the Company is required to complete CDD prior to establishing a new client relationship, and for existing clients will be based on the requirements set for remediation.

REQUIREMENTS FOR RISK BASED ASSESSMENT OF CLIENTS

To complete the risk-based assessment for each client, the Company must obtain, verify, and record certain identifying information.

In situations where the ownership or control arrangements of the client prevent the Company from identifying one or more of the client's beneficial owners, the Company will not establish a business relationship with that client.

Please notify the MLRO immediately (via email or telephone) where you doubt the accuracy and authenticity of documents provided by an existing client, if you suspect money laundering or if a change in circumstances of the client, warrants a change in the risk-rating of that client.

A copy of the Client Risk Assessment Form and the Guide to completing the form can be found within the Annexes.

III FINANCIAL RISK ASSESSMENT

1. Hoppacard d.o.o. applies the financial security measures (called in Directive 2015/849 as due diligence measures) indicated in this section.
2. Financial security measures include:
   a. identification of the Client and verification of his identity;
   b. identifying the Beneficial Owner and taking reasonable steps to:
      i. verification of his identity,
      ii. determine the ownership and control structure in the case of a Client that is a legal person, an organizational unit having no legal personality or a Trust;
   c. assessing the business relationship with Client and, as appropriate, obtaining information on its purpose and intended nature;
   d. ongoing monitoring of the Client's business relationships including:
      i. an analysis of transactions undertaken throughout the course of business relationships to ensure that the transactions are consistent with Hoppacard d.o.o.'s knowledge of the Client, the nature and scope of its business and consistent with the Money Laundering and Terrorist Financing risks related to that Client;
      ii. investigation of the source of origin of property values at the disposal of the Client - where justified by the circumstances;
      iii. ensuring that the documents, data or information in its possession relating to the business relationship with the Clients are kept up to date.
3. Financial security measures shall be applied in particular in the following cases:
   a. establishment of business relationships (conclusion of the Contract);
   b. carrying out Occasional Transactions:
      i. with a value of EUR 15 000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked (Related Transactions), or
      ii. which is a Transfer of Funds for an amount exceeding the equivalent of €1,000;
      iii.
   c. a suspicion of Money Laundering or Terrorist Financing;
   d. doubts about the accuracy or completeness of the Client's identification data obtained so far;

e. in relation to Clients with whom Hoppacard d.o.o. has a Contract, taking into account the identified risks of Money Laundering and Terrorist Financing, in particular when:
    i. there has been a change in the previously determined nature or circumstances of the business relationship;
    ii. there has been a change in the previously determined details concerning the Client or the Beneficial Owner;
    iii. Hoppacard d.o.o. was obliged by law during the calendar year in question to contact the Client in order to verify the information concerning the Beneficial Owners.

4. Where one of the measures of this Procedure cannot be applied, Hoppacard d.o.o.:
    a. does not establish business relationship (does not conclude a Contract);
    b. not carry out a Transaction, including an Occasional Transaction;
    c. dissolves business relationship (terminates the Contract).
5. Hoppacard d.o.o. assesses whether the inability to apply financial security measures, constitutes grounds for a notification to the GIIF about:
    a. of circumstances that may indicate the suspected commission of Money Laundering or Terrorist Financing offences; or
    b. the case of a reasonable suspicion that a specific Transaction or specific Property Value may be connected with Money Laundering or Terrorist Financing.
6. The financial security measures applied to the Client depend on the risk class assigned to the Client. The risk classes are described in section VIII of this Procedure.

Hoppacard d.o.o. documents electronically or in writing the financial security measures applied and the results of the ongoing analysis of the Transactions carried out, including by archiving copies or scans of documents, including identity documents, provided or received from the Customer.

3. DUE DILIGENCE PROCESS

Due to the nature of the business, enhanced due diligence will be conducted on all customers. Due diligence is conducted to identify the clients we are dealing with and where required verify their identity through legitimate documents and review them against the UN and other international sanctions lists.

Note that further EDD will be conducted on customers where they have been identified with high-risk factors for financial crime, however this is determined on a case-by-case basis. The Company will take an informed decision, agreed with the MLRO, about the level of enhanced due diligence measures are appropriate in each high-risk situation.

The Company's enhance due diligence measures include:

- verifying the identity of the client and any Beneficial Owners; and ● understanding the source of funds and source of wealth.

Beneficial Owners are natural persons who meet any of the criteria below:

  - own or control (whether directly or indirectly) more than 25% of the client's shares or voting rights;
  - has the right to appoint or remove a majority of the board of directors of a body corporate; or
  - has the right to exercise significant influence or control over the client.

- Increasing the quantity of information obtained for customer due diligence purposes:

i. About the customer's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the customer's or beneficial owner's reputation and assessing any negative allegations against the customer or beneficial owner. Examples include information about family members and close business partners; information about the customer's or beneficial owner's past and present business activities; and adverse media searches

ii. About the intended nature of the business relationship, to ascertain that the nature and purpose of the business relationship is legitimate and to help us obtain a more complete customer risk profile. It includes obtaining information on:

   a. the number, size, frequency and reason for the transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate

   b. the reason the customer is looking for a specific product or service, in particular where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction

   c. the destination of funds

   d. obtain and verify information on the intended nature of the business relationship; and

   e. conduct more regular reviews and updating of the CDD information that the Company holds;

   f. verification of the client's source of funds and source of wealth;

g. increased monitoring of the business relationship to determine whether there are any unusual or suspicious transactions

h. the nature of the customer's or beneficial owner's business to better understand the likely nature of the business relationship and obtain and verify additional identification information on the client and all beneficial owners;

iii. Monitoring IP addresses and conducting proximity analysis

- Increasing the quality of information obtained for customer due diligence purposes to confirm the customer's or beneficial owner's identity including by:

i. Requiring the first payment to be carried out through an account verifiably in the customer's name with a bank subject to Slovenia and European Union Customer Due Diligence standards

ii. Establishing that the customer's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with the Company's knowledge of the customer and the nature of the business relationship.

- Increasing the frequency of reviews, to be satisfied that the Company continues to be able to manage the risk associated with the individual business relationship and to help identify any transactions that require further review, including by:

- Obtaining the approval of the MLRO to commence or continue the business relationship to ensure senior management are aware of the risk the Company is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk

- Reviewing the business relationship on a more regular basis to ensure any changes to the customer's risk profile are identified, assessed and, where necessary, acted upon

- Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorist financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions

- The MLRO will need to provide approval, or refusal, to proceed with the customer set up process prior to conducting any business with a customer who has been through the enhanced due diligence process

The KYC information and transactions of all High-Risk clients are reviewed annually to ensure that we retain valid and up-to-date information and assess the client's actual transaction pattern against the declared or expected behaviour. As part of this exercise and where required, we also update information with regards to a client's source of funds and wealth and where needed increase the degree and nature of monitoring of the business relationship

The Management Body will consider its risk appetite in relation to customers. The MLRO may decide to reject existing or new customers on the basis of financial crime concerns. The Board of Directors will be informed, and the relevant customer closing procedure will be followed.

The process below describes the steps required to complete the CDD process.

3.1. PRIVATE INDIVIDUALS

3.1.1. IDENTIFYING PRIVATE INDIVIDUALS AS CUSTOMERS

The Company will obtain the following information for prospective customers that are individuals:

- Full name
- Current residential address
- Date of birth
- Nationality
- legal domicile
- Occupation
- Purpose of Account
- Expected Annual Transaction Activity

For nonface to face onboarding/due diligence the additional documents/information will be required:

A "selfie" of the individual together with two currently valid forms of the Client's facial ID; one must be the Client's passport with all details clear and visible, the second should be a copy (front and back) of an official government issued document, such as a national ID or driver's license.

3.1.2. VERIFYING IDENTITIES OF PRIVATE INDIVIDUALS

The Company will verify the information obtained using reliable and independent sources, either by viewing documentation from the customer or via electronic checks using the Company's third-party system Sumsub.

Acceptable documentary evidence provided by customers consists of: government issued documents with photos, such as valid passport, photo card driving licence or national identity card, or government issued documents without photos which incorporate the customer's full name and either their residential address or their date of birth. A signed self-certification from each client, identifying the details of all passports issued and held in their name(s) must be obtained

Electronic verification will include the customer's full name, address and date of birth and will be carried out by Sumsub, using a range of positive information sources, can access negative information sources and has a transparent process.

When electronic verification is used or a customer has not been physically present for identification purposes, the Company will carry out an additional verification check to manage the risk of impersonation fraud. This check may take the form of:

- Requiring the first payment to be carried out through an account in the customer's name
- Telephone contact with the customer on a home or business number that has been verified, prior to opening the account
- Communicating with the customer at the address that has been verified
- Requiring copy documents to be certified by an appropriate person

The Company will consider on a case-by-case basis any customers that cannot reasonably be expected to produce the standard evidence of identity and will seek to agree to the use of other confirmations of identity so that customers are not unreasonably denied access to the products and services.

Any exceptions to this policy will be recorded by the MLRO and maintained in a register which is reviewed at least annually.

3.2. CORPORATE CUSTOMERS

3.2.1. IDENTIFYING CORPORATE CUSTOMERS

The Company will obtain the following information for prospective customers that are private companies:

- Full name
- Trading name
- Registered number
- Registered address
- Trading address (if different from registered address)
- Shareholder structure
- Nature of business
- Expected Monthly Turnover
- Names and identification documents of all the directors
- Names and identification documents of individuals who own or control over 25% of its shares or voting rights
- Names of individuals who exercise control over the management of the company
- Names of ALL beneficial owners for Sanctions and PEP screening

The Company will take reasonable steps to identify the beneficial ownership and controllers of the corporate

3.2.2. VERIFYING IDENTITIES OF CORPORATE CUSTOMERS

The Company will verify the identity of the customer by confirming the company's listing on a regulated market (where relevant), searching the relevant company registry, viewing a copy of the company's Certificate of Incorporation. If there is a discrepancy between the company register and the customer information, then the Company will discuss the discrepancy identified requesting for confirmation of the correct information and update where confirmation by the client has been provided.

The Company will also ensure that anyone acting on behalf of the customer is authorised to do so and will identify and verify the identity of that person.

3.3 POLITICALLY EXPOSED PERSONS (PEP)

Politically exposed persons ("PEPs") here include a Natural Person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, including but not limited to, a head of state or of government, senior officials and functionaries of an international or supranational organisation, senior politician, senior government, judicial or military official, ambassador, senior executive of a state owned corporation, or an important political party official.

Consequently, the Company conducts EDD where PEPs are directors or beneficial owners of a client. Where a PEP is identified as Beneficial Owner, enhanced due diligence (EDD) will be applicable. PEPs can pose a higher money laundering risk to Company's as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status

itself does not, of course, incriminate individuals or entities, however, it does put the customer, or the beneficial owner, into a higher risk category.

Where the Company specifically deals with PEPs of the USA, it will comply with the provision of the Foreign and Corrupt Practices Act (1977) (FCPA). *Note the Company does not onboard US residents, however there could be cases of dual nationality, where a US national is residing in the Slovenia and European Union.*

The Company will check all customers at the initial account set up and at least annually to identify any PEPs, using World Check and Sumsub Online or another source. If a PEP is identified, the MLRO will be notified, and enhanced due diligence measures will be employed.

Factors that will be considered in assessing the level of risk posed by the PEP include but are not limited to:

- Geographic location
- Official responsibilities of the individual and their office
- Nature of their title (i.e. whether it is honorary or salaried)
- Level and nature of authority or influence over government activities or other officials
- Access to significant government assets or funds
- Source of wealth and source of funds to be used for the transaction
- If the PEP is a beneficial owner or director of a corporate client, the type and extent of influence or control the PEP has over the direction of that corporate

Once due diligence is complete, approval will be sought from the MLRO with the final approval by Senior Management; prior to the commence a business relationship with the customer

Where approval is granted to continue with the PEP relationship the reasoning will be documented by the MLRO and the nature and extent of the on-going monitoring of the account will be agreed with the relevant teams in the Company. The first payment must be carried out through an account in the customer's name with a financial institution that is subject to money laundering regulation and supervision in a jurisdiction that has standards equivalent to those set out in the FATF Recommendations. The name of the PEP will be added to the Company's PEP register.

Where approval is not granted to continue with the PEP relationship, the MLRO, in liaison with the relevant teams, will ensure that any identifiable money laundering risk is assessed and dealt with appropriately, the customer relationship is ended.

The Company will maintain a register of PEPs which will be regularly reviewed (at least annually) by the MLRO.

3.4 Sanctions and Adverse News Screening

In addition to PEP screening, the Company undertakes sanctions and adverse news screening at the time of onboarding and on a daily basis. The company has zero tolerance to sanctions using the database of external provider Sumsub. It screens both senders and beneficiaries. Adverse news is analysed on a risk sensitive basis with the decision subject to MLRO approval

3.5 Nature of Business

The Company will obtain and record sufficient information on the customer's nature of business and the purpose of the account, including expected source of funds, source of wealth and anticipated transaction volumes and values. This will enable an assessment of whether the purpose of the account to be opened is consistent with the nature of business.

3.6 Simplified Due Diligence (SDD)

3.7 Ongoing Monitoring

The Company will monitor its customers for signs of money laundering on an ongoing basis, focusing on transaction monitoring and customer reviews. All customers, their businesses, and transactions will be reviewed against all Sanctions Lists (locally and internationally). When undertaking on-going CDD the Company must, using the risk-based approach:

i. monitor transactions to ensure they are consistent with the Company's knowledge of the Customer, his business and risk rating;

ii. pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

iii. enquire into the background and purpose of the transactions;

iv. periodically review the adequacy of the CDD information it holds on Customers and Beneficial Owners to ensure that the information is kept up to date, particularly for Customers with a higher risk rating; and

v. periodically review each Customer's risk assessment to ensure that its risk rating remains appropriate in light of current money laundering risks.

Such reviews must be carried out when:

i. the Company changes its CDD documentation requirements;

ii. an unusual transaction with the Customer is expected to take place;

iii. there is a material change in the business relationship with the Customer; or iv. there is a material change in the nature or ownership of the Customer.

3.8 RED FLAGS

Red flags are customer behaviours or issues with customer's business that should act as a warning that further investigation by the Company is necessary.

Examples of red flags are:

- Customer is reluctant to provide information or is evasive
- Customer's lifestyle appears in excess of known sources of income
- Customer's business structure is unnecessarily complicated
- Involvement of third parties without valid reason
- Unusual instructions
- Repeated or inexplicable changes to instructions
- Use of bank accounts without valid reason
- Complex structuring of transactions without valid reason
- Customer's disinterest in prices, commissions, costs etc.
- Transactions out of line with expected transaction for the customer
- Unexplained transfers of funds

If any red flags are identified in the Customer Due Diligence or monitoring processes, employees must notify the MLRO immediately.

4. TRANSACTION MONITORING

Based on the Company's knowledge of the customer, the monitoring will look for:

- Unusual behaviour - sudden and/or significant changes in transaction activity by value, volume or nature, such as change in beneficiary or destination
-
-
- High risk geographies and entities - significant increases of activity or consistently high levels of activity with higher risk geographies and/or entities
- Other money laundering behaviours – indications of possible money laundering, such as the structuring of transactions under reporting thresholds, transactions in round amounts, overly complex transactions
- Dormant relationships

Where unusual patterns are identified, then enhanced due diligence will be carried out. Enhanced due diligence will include:

- Establishing the source and destination of the funds being used to fund these transactions and the customer's source of wealth more broadly
- Finding out more about the customer's business to understand the rationale and reason for the transactions
- Monitoring the business relationship and subsequent transactions more frequently on a weekly or even daily basis if necessary.

Any suspicious activity will be reported to the MLRO for further investigation and/or reporting to the necessary authorities.

The Company uses a combination of manual and automated transaction monitoring. The methods of transaction monitoring will be dependent on the size and nature of the Relevant Person's business and customer base and the complexity and volume of customer transactions. The Company determines appropriate thresholds in accordance with the risk rating of the customer in conjunction with the customer risk assessment and Business Wide Risk Assessment.

4.1. KYC Refresh

The Company will ensure that customer due diligence information is relevant and kept up to date via regular customer reviews. The extent to which customer reviews are undertaken will be determined using a risk-based approach and applied in accordance with the risk rating applied to the customer during the customer risk assessment.

The Company has a customer review process based on the high-risk factors assigned to its customers.

4.1.1. Re-verification of identification

Once the identity of a customer is satisfactorily verified, there will usually be no need to re-verify identity, unless the customer's name changes, the beneficial ownership or control changes materially, subsequent doubts arise as to the accuracy of evidence previously obtained or a new risk emerges.

On an annual basis, all customers will undergo a complete review. This will entail establishing the following:

- Re-confirmation of Address
- Re-confirmation of Corporate Structure (if applicable)
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

4.1.2. Trigger events

In addition to the scheduled review above, if the Company, through the course of its daily activities, obtains information that brings question to the accuracy of the customer due diligence information collected, or if a suspicion arises, then the customer will undergo an immediate review, irrespective of their risk status.

4.2. MLRO REVIEWS

The MLRO will conduct regular independent reviews on all or a sample of all accounts opened to ensure that the correct level of due diligence was performed. Accounts will be checked to ensure that the appropriate documentation was obtained, a business profile was established, the customer was checked for PEPs and Sanctions, and that the customer activity matches the expectation from the business profile.

The MLRO will investigate any discrepancies and share any findings with the relevant employees.

5. Suspicious Activity Reporting

Employees are expected to be alert to money laundering, and they are responsible for reporting any actual or suspected money laundering to the MLRO in a timely manner. Reporting is to be done via the Internal Suspicious Activity Report.

Examples of such circumstances are (but limited to):

- Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;
- Transactions requested by a Person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a Relevant Person in relation to a particular customer;
- where the size or pattern of Transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or may have been deliberately structured to avoid detection; (d) a customer's refusal to provide the information requested without reasonable explanation;
- where a customer who has just entered into a business relationship uses the relationship for a single Transaction or for only a very short period of time;
- an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

5.1. INTERNAL SUSPICIOUS ACTIVITY REPORTING

As mentioned above, all suspicions should be reported to the MLRO via the Internal Suspicious Activity Report. The Report is to include clear details of the suspected activity(ies).

Suspicions may be reported informally to the MLRO by email, phone or in person but must be followed up with a signed and dated Internal SAR Form or can be requested from the MLRO. The Internal SAR Form provides documentary evidence that the employee has fulfilled their personal obligation to report a suspicious transaction.

Note that employees must not discuss their suspicions, evidence or grounds for suspecting a transaction may be deemed suspicious with any person other than the MLRO. This includes fellow employees and the customer to avoid tipping off.

The MLRO will discuss with employees what to say to customers and how to deal with enquiries about why their account are frozen automatically in order to avoid tipping off.

5.2. External Suspicious Reporting

Where the MLRO receives a Suspicious Activity Report, he must start the investigation within 24 hours of receiving such notification. The investigation may include reviewing the KYC forms, interviewing the relevant employees and reviewing client transactions history or any other information the MLRO considers appropriate;

Based on the results of the investigation completed, the MLRO is to determine if to file an SAR/STR with the Slovenia Financial Intelligence Unit (FIU), in accordance with AML Legislation and the applicable relevant regulations, laws and decrees. The MLRO's decision to make an external SAR is made independently and is not subject to the consent or approval of any other Person.

In any case, the MLRO must immediately notify the FIU when he becomes aware of any situation where:

I. Carrying on or about to carry on a service;

II.

III. Undertaking or about to undertake any other business whether or not arising from or in connection with (i) or (ii);

where such carrying on, holding or undertaking constitutes or may constitute a suspicion of money laundering or a contravention of a relevant sanction or resolution issued by the UN Security Council. When the MLRO does that, he must freeze the transaction for at least 96 hours pending when he receives feedback from the FIU. The FIU may either give a clearance for him to either proceed with the transaction or may instruct him to freeze the funds for a maximum of six months. The FIU may further renew the six months freeze once before it expires.

The notification must include a description of the relevant activity, and the measures proposed to be taken or that has been taken by the Company with regard to the matters specified in the notification.

Reasonable measures include, but are not limited to:

i. requiring specific elements of enhanced CDD;
ii. requiring enhanced reporting mechanisms or systematic reporting of financial transactions;
iii. limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;
iv. prohibiting the Company from relying on third parties located in a specified jurisdiction to conduct CDD;

If there are concerns about any repercussions of making a SAR, then the Whistleblowing Policy and Procedure should be followed for information on alternative methods of making a report.

If decision not to file the SAR/STR is made, full details of the rationale for this decision will be kept on record.

Failure to notify an appropriate person about criminal actions of which an employee is or should have been aware, in breach of this policy, may be considered to be a contractual breach leading to disciplinary actions or personal criminal liability.

5.3. SUBSEQUENT INVESTIGATIONS

The Company is committed to supporting regulators and law enforcement officers in the prevention of financial crime.

All employees are expected to cooperate fully with any investigations. Employees must also recognise, however, that laws and procedures may apply to the disclosure of information, and they should therefore contact the MLRO before disclosing information about customers or employees when contacted directly by law enforcement officers.

6. BANK TRANSFERS

6.1. SENDING OR RECEIVING FUNDS

When the Company sends or receives funds by wire transfer for a Customer, the following needs to be taken into account:

- ensure that the wire transfer and any related messages contain accurate originator and beneficiary information;
- ensure that, while the wire transfer is under its control, the information in (i) remains with the wire transfer and any related message throughout the payment chain;
- monitor Bank Transfers for the purpose of detecting those Bank Transfers that do not contain both originator and beneficiary information and take appropriate measures to identify any money laundering risks; and
- not effect Bank Transfers without the information required under as outlined in 14.2;

6.2. INFORMATION ACCOMPANYING BANK TRANSFERS

A. The Company must ensure that all Bank Transfers contain the following information, at a minimum.

- the name of the originator;
- the originator account number where such an account is used to process the Transaction or unique Transaction reference number if no originator account number exists;
- the originator's address, or national identity number, or customer identification number, or date and place of birth;
- the name of the beneficiary; and
- the beneficiary account number where such an account is used to process the Transaction or unique Transaction reference number if no beneficiary account number exists.
- If the Company undertakes batch transfers its must:
- verify the originator information and;
- the batch file contains the beneficiary information for each beneficiary and that the information is fully traceable in the beneficiary's jurisdiction.

7. RECORD KEEPING

Records relating to the verification of a customer's identity required for the due diligence process will be retained for a period of 5 years from the date on which the notification or report was made, the business relationship ends, or the Transaction is completed, whichever occurs last, after which the personal data will be destroyed, in order to uphold the customer's data protection rights. A further period of retention, not exceeding 5 years, may be permitted if after a thorough assessment, the Company believe this is justified for the prevention, detection or investigation of money laundering.

The Company will keep the following records for a period of 5 years minimum:

- Transaction records (carried out with or for a customer)
- Records of any internal reports made to the MLRO and of any external SAR reports made by the MLRO (from the date on which the report was made).
- Where the MLRO has considered information or other matter concerning knowledge or suspicion that another person has engaged in money laundering, but has not made a report to the FIU, a record of that information must be kept at the Company's offices and the MLRO is responsible for ensuring that these records are complete and up to date

Where customer records are kept by the Company outside the Slovenia, the Company must ensure records are kept in a manner consistent with the PFSA rules. If records are held outside the Slovenia the Company must verify whether there is relevant legislation that would restrict access to customer records by either the Company, the PFSA or law enforcement agencies of Slovenia. Where such legislation exists, the Company must ensure it retains certified copies of relevant identification information in an accessible jurisdiction.

8. Sanctions And Other International Findings

8.1. Government, Regulatory and International Findings

The Company has systems and controls to ensure that on an ongoing basis it is properly informed in relation to any sanctions or other international findings issued by the following bodies:

Slovenian Regulator

List Name	Description	Source
Slovenian Overview of Restrictive Measures (Omejevalni ukrepi)	Central gov.si hub explaining how sanctions are implemented in Slovenia under national law and EU/UN acts. It points to the continuously-updated EU financial sanctions list and UN lists.	www.gov.si "Restrictive measures" (EN/SI).
Bank of Slovenia — Financial Restrictive Measures	Supervisory guidance for banks/payment institutions on implementing financial sanctions (screening, asset freezes, reporting).	www.bsi.si
ATVP Public Warnings (Opozorila)	Warnings from the Slovenian Securities Market Agency about firms/individuals operating without required authorisation or breaching capital markets rules (Slovenia's analogue to KNF public warnings).	https://www.a-tvp.si/

Polish Regulator

List Name	Description	Source
Polish National Sanctions List (Krajowy Wykaz Sankcyjny)	A national list maintained by the Polish Ministry of the Interior and Administration. It includes individuals, entities, and organizations subject to sanctions under Polish law.	Ministry of the Interior and Administration
Warnings and Alerts from the Polish Financial Supervision Authority (KNF)	The KNF issues warnings about unauthorized financial market participants and maintains a list of entities operating without proper authorization or in violation of Polish financial regulations.	KNF Public Warnings
Lists Related to Tax Offenses	The Polish Ministry of Finance maintains records of entities involved in tax offenses, relevant for AML/CTF efforts.	Ministry of Finance

EU and International Sanctions and High-Risk Lists

List Name	Description	Source
EU Consolidated List of Sanctions (Sanctions Map)	A comprehensive list of individuals, groups, and entities subject to EU financial sanctions.	EU Sanctions Map
EU List of High-Risk Third Countries	Countries identified by the European Commission with strategic deficiencies in their AML/CTF regimes.	European Commission - High-Risk Third Countries
Financial Action Task Force (FATF) Lists	**High-Risk Jurisdictions Subject to a Call for Action**: Countries with significant AML/CTF deficiencies.	FATF High-Risk Jurisdictions
	Jurisdictions under Increased Monitoring: Countries working with FATF to address deficiencies.	
United Nations Security Council Consolidated List	Individuals and entities subject to UN sanctions measures.	UN Security Council Consolidated List
EU List of Non-Cooperative Jurisdictions for Tax Purposes	Countries that do not meet EU tax transparency and fair taxation criteria.	EU List of Non-Cooperative Jurisdictions
EU Counter-Terrorism Sanctions List	Targeted sanctions against individuals and entities involved in terrorism.	EU Terrorist List

Additional Beneficial and Optional Lists

List Name	Description	Source
Interpol Red Notices	Notices issued for individuals who are wanted for extradition.	Interpol Red Notices
World Bank Listing of Ineligible Firms & Individuals	Entities and individuals debarred from World Bank-financed contracts due to fraudulent or corrupt practices.	World Bank List of Ineligible Firms & Individuals
EUROPOL Reports and Watch Lists	Information on criminal activities and organizations within the EU.	EUROPOL
National Sanctions Lists of Other Countries	**UK Sanctions List**: Post-Brexit sanctions regime of the UK.	**UK Sanctions List**: UK Government Sanctions
OFAC	**U.S. OFAC Sanctions Lists**: Relevant for USD transactions or U.S. persons.	**OFAC Sanctions Lists**: U.S. Department of the Treasury - OFAC

Basel Committee on Banking Supervision Publications	Guidelines on banking regulations and AML/CTF practices.	Basel Committee on Banking Supervision
Wolfsberg Group Guidance	Provides AML/CTF guidelines widely adopted in the financial industry.	The Wolfsberg Group
Commercial Risk Intelligence Databases	Databases compiling various sanctions lists, PEPs, and adverse media.	**LSEG (Refinitiv) World-Check**: World-Check
Dow Jones Risk & Compliance	Provides data, tools, and technology to help businesses manage risks related to regulatory compliance, financial crime, and reputational exposure	**Dow Jones Risk & Compliance**: Dow Jones Risk & Compliance
Local and International Law Enforcement Alerts	Bulletins and alerts about emerging threats from law enforcement agencies.	Europol, Interpol, National agencies
Non-Governmental Organization (NGO) Reports	Reports from organizations like Transparency International on corruption risks.	Transparency International

Regulatory Guidelines and Directives

List/Guideline	Description	Source
EU Anti-Money Laundering Directives (AMLD)	Frameworks outlining AML/CTF measures, including references to PEPs and high-risk countries.	European Commission - AML Directives
European Central Bank (ECB) Guidelines	Regulatory guidelines that may include lists relevant to financial compliance.	European Central Bank (ECB)
European Banking Authority (EBA) Guidelines	Regulatory guidelines that may include lists relevant to financial compliance.	European Banking Authority (EBA)

Key Actions for Compliance

- **Regular Updates:** To ensure all lists are updated promptly to reflect the latest changes. Automated systems can help in real-time updates.
- **Integrated Screening:** Utilize compliance software to integrate these lists into transaction monitoring systems for efficient screening.
- **Employee Training:** Regularly train staff on compliance requirements and updates to these lists to ensure awareness and proper implementation.
- **Policy Reviews:** Periodically review internal policies and procedures to align with regulatory changes and best practices.
- **Enhanced Due Diligence (EDD):** To apply EDD measures for transactions involving high-risk countries, PEPs, or entities on any of the above lists.

9. Notifications

The Company must notify the PFSA in writing as soon as possible if during its activities or the activities of any Branches or Subsidiaries applicable to it:

I. receives a request for information from another regulator responsible for AML or Sanctions regarding enquiries into potential money laundering, terrorist financing or Sanctions breaches;

II. becomes aware of or has reasonable grounds to believe that the following has or may occur, money laundering (contrary to Federal Law), Sanctions breaches or acts of Bribery;

III. is aware of any money laundering or Sanctions issue that could affect the Company or a member of its Group resulting in reputational damage;

IV. is aware of any significant breach of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism No.1 by either the Company or any employee.

10. Breaches of Anti-Money Laundering Policy

Any breaches of the Anti-Money Laundering rules will be recorded on the Company's AML Breach Log in conjunction with its Regulatory Breach Policy to GIFI (General Inspector for Financial Information).

PART 3 APPENDICES

APPENDIX 1 - SOURCE OF FUNDS (SOF)

Description of source of funds	Details required	Documentary Evidence required (original or fully certified copy)
1. Income-savings from salary (basic and/or bonus)- if self-employed or company share owner refer to 4 below	All of the following: ● Salary per annum ● Employer's name and address ● Nature of Business	Two of the following: Payslip (or bonus payment) from the last three months Letter from employer confirming salary on letterheaded paper Bank statement showing clearly showing receipt of most recent regular salary payments from named employer
1. Sale of investment/liquidation of investment portfolio	All of the following: ● Description of shares/units/deposits ● Name of seller ● How long held ● Sale amount ● Date funds received	One of the following: ● Investment/savings certificates, contract notes, or surrender statements ● Bank statements clearly showing receipt of funds and investment company name ● Signed letter detailing funds from a regulated accountant on letter –headed paper.
2. Sale of Property	All of the following: ● Sold property address ● Date of Sale ● Total sale amount	One of the following: ● Letter form a licenced solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of purchaser ● Copy of Sale contract
3. Company Sale	All of the following: ● Name and mature of the company ● Date of Sale ● Total sale amount ● Customer's share	● Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter headed paper. ● Copy of contract of sale, plus bank statement showing proceeds ● Copies of media coverage (if applicable) supporting evidence

4. Inheritance	All of the following: ● Name of deceased ● Date of death ● Relationship to customer ● Date received ● Total amount ● Solicitors' details	One of the following: ● Grant of probate (with a copy of the will) which must include the value of estate ● Copy of will ● Letter from lawyer or trustee
5. Divorce settlement	Date and total amount received Name of divorced partner	One of the following: ● Copy of the court order ● Letter detailing divorce settlement signed by a licensed solicitor on letter headed paper
6. Company profits	All of the following: ● Name and address of the company ● Nature of company ● Amount of annual profit	One of the following: ● Copy of the latest audited company accounts ● Confirmation of the nature of business activity and turnover detailed in a letter from a regulated accountant
7. Retirement income	All of the following: ● Retirement date ● Details of previous occupation/profession ● Name and address of the employer ● Details of pension income source	One of the following: ● Pension statement ● Letter from a regulated accountant ● Bank statement showing receipt of latest pension income and name of provider ● Savings account statement
8. Fixed Deposits/Savings	All of the following: ● Name and institution where savings account is held ● Date the account was established ● Details of how the savings were acquired	All of the following: ● Savings statement ● Evidence of account start (letter from the account provider) ● Additional evidential information can be requested in relation to the origin of the savings held.
9. Dividend payments	All of the following: ● Date of receipt of dividend ● Total amount received ● Name of company paying dividend ● Length of time the shares have been held in the company	One of the following: ● Dividend contract note ● Bank statement clearly showing receipt of funds and name of company paying dividend If dividend is payable from the customer's own company, one of the following: ● Letter detailing dividend details signed by a regulated accountant on letter headed paper

		● Set of company accounts showing the dividend details
10. Gift	● Details of date and amount of gift ● Details of person making gift – ID and occupation details for PEP/Sanctions screening ● Reason for gift and the nature of the relationship to the individual making the gift	● Letter from donor confirming details of gift ● If PEP Documented evidence of donor's source of wealth as laid out in this table
11. Loan	● Name of loan provider ● Date and amount of loan	● Copy of the Loan Agreement and details of any security or, ● Copy of loan statements
12. Lottery/Gambling Win	● Name of source ● Details of Windfall	● Evidence from the lottery company ● Cheque ● Winnings' receipt
13. Compensation Pay-out	● Details of events leading to claim	● Letter/court order from compensating body or ● Solicitor's letter
14. Life Insurance/general insurance pay-out	● Amount Received ● Policy Provider ● Policy Number/reference ● Date of pay-out	● Pay-out statement ● Letter from insurance provider confirming pay-out

Source of Virtual Assets	Samples
Virtual Assets purchased on other brokers and other exchanges	• Screenshots of purchase and withdrawal confirmation displaying your account ID and all transaction details; OR • Confirmation emails which provide proof of purchase or withdrawal; OR • Receipts which provide proof of purchase (e.g. using an OTC)
Income from Services (e.g. affiliate income or other services)	• Detailed description of the service; AND • Receipts for services which have been paid for in Virtual Assets; AND • Names, addresses, contact details and information about the companies involved, as well as their legal form; AND • Virtual Asset addresses of the sender and the recipient; AND • Transaction IDs (hash); AND • The amount sent, displayed in both virtual assets and fiat; AND • Date of the transaction; AND • Bank statements displaying both receipts and transactions; AND • A screenshot of your wallets, which show their current income; AND • Screenshots of your transaction history and withdrawal history; AND • Explanations of the origin of the virtual assets used for the payment transactions.

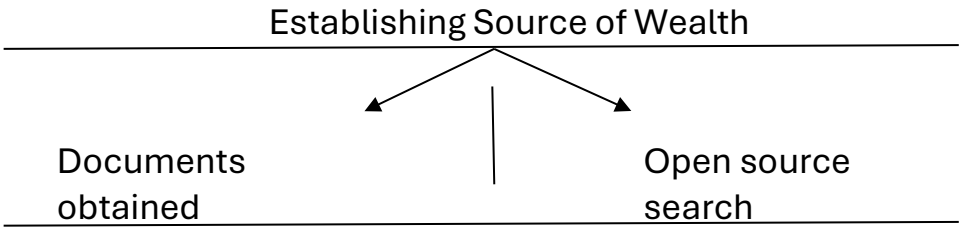
Initial Coin Offering (ICO)	• Copy of contract confirmation payment made in virtual asset; AND • Full name of the ICO and associated project's website must be visible along with exact amount invested in the virtual asset; AND • Transaction history documents that purchase and withdrawal of the token (wallet addresses and transaction ID); AND • Bank statement, if a fiat currency was used for investing; AND • Confirmation emails, which display the purchase.
Mining	• Receipts for the purchase of mining hardware, on which the address of the buyer (the name that you have registered on Hoppacard d.o.o.), and seller are displayed. If your address has changed in the meantime, please provide proof that you lived or worked at that address at the time of purchase; AND • Photos of mining hardware and screenshots of the platforms and programs used; AND • Screenshots of mining revenues and rewards; AND • Screenshots of displaying transaction history from and to wallets, which display wallet addresses and transaction IDs (self-made "excel lists cannot be accepted); AND • If coins from mining activities have also been traded, screenshots displaying the transaction history are needed, which clearly display receipt on the respective exchange and the name of the account holder. Furthermore, all trades must be clearly identifiable and must not be mixed with trades of other coins - e.g. customer can highlight
Airdrops	• Screenshots of the transaction history, on which the deposits and withdrawals of Hoppacard d.o.o. are visible; AND • Wallet addresses and transaction IDs

Coin or Token swaps	● If the token name or the number of tokens has changed due to so-called coin swaps or token swaps or other technical changes (e.g. redenomination) to the blockchain or platform which has been used, please provide screenshots of the transaction history (wallet addresses and transaction IDs)
Lending or Liquidity pools	● If a matter of lending income is involved, please prove this by means of screenshots of the transaction history (wallet addresses and transaction IDs). It must clearly highlight where the deposited assets have been placed as collateral, in what amount and where the collateral that is being used has come from.

Notes:

- All documents provided by customers should show their name clearly, date and amount
- The Source of funds document should reflect the recent transactional activities in question

APPENDIX 3 - SOURCE OF WEALTH (SOW)



Source of Wealth	**Examples** *(non-exhaustive list)*
Family/Generational wealth and personal background	● Inheritance ● Gifts (from family including spouse/partner) ● Divorce settlement ● Lawsuit settlement ● Pension ● Retirement benefit scheme pay-outs ● Lottery wins ● Real Estate owned ● Artwork
Total Income, Revenue and Business Activities	● Business ownership ● Employment ● Sales of products ● Business properties ● Bonuses ● Commissions ● Retirement scheme ● Salary
Investment Activities	● Acquisitions ● Sale of investments e.g. securities, royalties, patents etc.

APPENDIX 4 – ONBOARDING REQUIREMENTS

ONBOARDING GUIDELINES

INDIVIDUAL ONBOARDING

Required Documents
☐ Proof of identity – electronic ID verification (Valid EID for Slovenia and European Union citizens) ☐ Signed Self Certification Identifying details of all passports held ☐ Proof of address (mostly dated within the last 3 months) ☐ Source of Funds/Evidence of nature of business for sole traders
Source of Funds / Wealth (such as payslips, bank statements, investment certificates, completion statements evidencing property sales, evidence of inheritance, tax returns) on a case-by-case basis at the point of transaction.

Examples of Acceptable Documents	
Proof of ID	**Proof of Address**
☐ Current valid passport ☐ National Identity Card	☐ Current valid driving licence ☐ Council tax bill / demand letter * ☐ Bank statement/Credit Card Statement ** ☐ Utility Bill** ☐ Correspondence from Government Agencies *
** Must be the most less than 12 months old. ** Must be less than 3 months old*	

Document Translation
All non-English documents must be translated and certified. When dealing with low-risk jurisdictions it is usually sufficient for the Certifier to translate the document being used as evidence of identity or address (assuming they are qualified to do so). This must include: ☐ Provider of Issuing Document (Agency / Company / Authority) ☐ Document Type ☐ Issue Date ☐ Expiry Date (if applicable) ☐ Full Name (and appropriate Titles) ☐ Address ☐ Other details or information relevant to the document

CORPORATE ONBOARDING

Table 1: Required Documents
☐ Application form with list of authorised signatories ☐ Executed Board Resolution authorising the opening of the account and naming the signatories ☐ Certificate of Incorporation and any name change certificates (if applicable) ☐ Certificate of Incumbency (where applicable) ☐ Articles of Association ☐ Confirmation Statement (Shareholder and Director registers) ☐ Most recent Annual Accounts (audited if available) ☐ Proof of trading address if it differs from registered address (bank statement/utility bill) ☐ Proof of identity and address for all beneficial owners with 25% or more interest. Where nobody holds up to 25%, we will reduce the threshold to10% or lower until we have a majority, and we will obtain documents on the UBO or UBO's involved except where it is a quoted company ☐ Proof of identity and address for two Directors ☐ Proof of identity and address for authorised signatories/traders ☐ Evidence of nature of business (e.g. website) *Source of Funds / Wealth – This is usually peculiar to the business type, and this would have been assessed at the point of onboarding – This includes audited accounts and company vintage information usually obtainable from companies house, bank statements, details of source of sales proceeds and funds received at the point of transaction. We ensure we have a clear understanding of the nature of the client's business and hence the source of proceeds and the volume of such proceeds.*

OTHER ENTITIES ONBOARDING

Requirements for Onboarding Trusts	
Details to be recorded and maintained	☐ Full name of Trust. ☐ Nature and purpose of Trust (e.g. discretionary, testamentary, bare). ☐ Slovenia of establishment. ☐ Name of settlor(s) ☐ Names of all trustees. ☐ Names of any beneficial owners or class of beneficiaries. ☐ Name of any protector or controller.
Documentary evidence required to verify legal purpose	☐ Scheme Trust Deed or Founding Document ☐ Latest Deed of Appointment, listing all current Trustees (if Trustees have changed since establishment)
Additional	☐ Names, addresses and dates of birth and identity verification required for trustees in whose names an investment is registered (i.e. if trustee is a private individual, personal identity and address verification also required). ☐ Names and confirmation of the identity of any other trustees, names and addresses and confirmation of the identity of any protector or controller, plus names and verification of identity of any nominated beneficiaries or any beneficiaries to have received benefit in a class of beneficiaries.

Requirements for Partnership / Incorporated Body	
Details to be recorded and maintained	Business address. Names of all partners/principals who exercise control over the management of the partnership.
	Names of individuals who own or control over 25% of its capital or profit, or of its voting rights.
Documentary evidence required to verify legal purpose	Partnership deed showing rights and duties of the partners. Where applicable the most recent amendment to partnership deed that confirms the current partners. (Where there is no partnership deed, the provisions of the Partnership Act of the relevant jurisdiction shall apply) and the Head of Compliance will interpret and authorise.
Additional	Name, address, date of birth and identity verification is required for partners or owners with over 25% of shares with capital or voting rights. This can be lowered to enable us to get at least 75% of the holdings

Requirements for Charities	
Details to be recorded and maintained	▯ Nature of body's activities and objects. ▯ Names of all trustees (or equivalent). ▯ Names or classes of beneficiaries. ▯ Charity number and evidence of registration
Documentary evidence required to verify legal purpose	Charities have their status because of their purposes and can take several legal forms and evidenced as such. Companies limited by guarantee can be verified on the relevant jurisdiction's companies house registry with certificate of incorporation and most recent annual return ▯ Copy of Trust Deed ▯ All registered charities will be listed on the charities register of the Slovenia and should be confirmed as such. For example: ▯ England and Wales (http://apps.charitycommission.gov.uk/ShowCharity/RegisterOfCharities/AdvancedSearch.aspx) ▯ Scotland (http://www.oscr.org.uk/charities/search-scottishcharity-register)
	▯ Northern Ireland (http://www.charitycommissionni.org.uk/charity-search/) ▯ Names, addresses, dates of birth and identity verification required for the trustees/officers in whose name's investments are registered. ▯ Trustees/Officers should have appropriate authority to operate an account or give instructions concerning the use or transfer of funds or assets (for private individuals, personal identity and address verification is required). The onboarding of any charity represents a high risk and will be subject to approval by the Head of Compliance.
Charities present a very high risk and will be considered on a case-by-case basis with the approval of the MLRO. Frontline staff are thus advised to obtain a preliminary assessment/ approval from the MLRO for a specific charity and jurisdiction before proceeding with marketing efforts.	

Complete list of authority and regulatory bodies for Europe:

Country	Regulatory Body	Website
Austria	Federal Ministry of Social Affairs, Health, Care and Consumer Protection	sozialministerium.at
Belgium	Federal Public Service Justice	http://just.fgov.be
Bulgaria	Central Register of Public Benefit Organizations	http://justice.government.bg
Croatia	Office for Cooperation with NGOs	udruge.gov.hr
Cyprus	Ministry of Interior	moi.gov.cy
Czech Republic	Ministry of Justice	justice.cz
Denmark	Danish Business Authority	erst.dk
Estonia	Estonian Tax and Customs Board	emta.ee
Finland	Finnish Patent and Registration Office	http://prh.fi
France	Ministry of the Interior	http://interieur.gouv.fr
Germany	Federal Office of Administration	http://bva.bund.de
Greece	Ministry of Finance	minfin.gr
Hungary	National Office for the Judiciary	birosag.hu
Ireland	Charities Regulator	charitiesregulator.ie
Italy	Ministry of Labour and Social Policies	lavoro.gov.it
Latvia	Register of Enterprises	ur.gov.lv
Lithuania	Centre of Registers	registrucentras.lt
Luxembourg	Ministry of Justice	http://mj.public.lu
Malta	Office of the Commissioner for Voluntary Organisations	voluntaryorganisations.gov.mt
Netherlands	Chamber of Commerce	kvk.nl
Poland	National Court Register	http://krs.ms.gov.pl
Portugal	Institute of Social Security	seg-social.pt
Romania	Ministry of Justice	just.ro
Slovakia	Ministry of Interior	minv.sk
Slovenia	Ministry of Public Administration	gov.si
Spain	Ministry of Social Rights and 2030 Agenda	http://mptfp.gob.es
Sweden	Swedish Tax Agency	skatteverket.se

List of authority and regulatory bodies for UK:

List	Regulatory Body	Website
UK Sanctions List	A consolidated list of financial sanctions targets in the UK, including individuals and entities subject to asset freezes.	UK Government Sanctions List
Office of Financial Sanctions Implementation (OFSI) Guidance	OFSI provides guidance on financial sanctions, including updates on changes to sanctions regimes.	OFSI Guidance
Financial Conduct Authority (FCA) Warning List	A list of firms and individuals that the FCA believes are operating without its authorization.	FCA Warning List
HM Treasury Sanctions Notices	Official notices regarding changes to UK sanctions regimes.	HM Treasury Sanctions Notices
National Crime Agency (NCA) Alerts	Updates on serious and organized crime threats within the UK, including money laundering risks.	NCA Alerts news NCA Industry specific alerts

UK Regulatory Guidelines and Directives

List/Guideline	Description	Source
UK Money Laundering Regulations	UK's primary AML/CTF legislation implementing EU directives.	UK Legislation - Money Laundering Regulations
Financial Conduct Authority (FCA) Guidelines	Regulatory guidelines on AML/CTF compliance for financial institutions.	FCA AML Guidance
Joint Money Laundering Steering Group (JMLSG) Guidance	Industry-led guidance on compliance with AML/CTF regulations.	JMLSG Guidance
National Risk Assessment of Money Laundering and Terrorist Financing	Government assessment identifying domestic high-risk areas.	UK National Risk Assessment

United States of America (USA)

Specific list by U.S: Regulators

List Name	Description	Source
Specially Designated Nationals and Blocked Persons List (SDN List)	OFAC's primary sanctions list including individuals and entities owned or controlled by targeted countries or associated with terrorism or other threats.	OFAC SDN List
Consolidated Sanctions List	Includes various OFAC sanctions lists such as the Foreign Sanctions Evaders List, Sectoral Sanctions Identifications List, etc.	OFAC Consolidated Sanctions List
Bureau of Industry and Security (BIS) Entity List	Entities restricted from receiving U.S. exports of goods and technology.	BIS Entity List
Denied Persons List	Individuals and entities denied export privileges by the BIS.	Denied Persons List
Federal Bureau of Investigation (FBI) Most Wanted Lists	Lists of individuals wanted by the FBI for various crimes, including terrorism.	FBI Most Wanted
Financial Crimes Enforcement Network (FinCEN) Advisories	Advisories on AML/CTF issues, including updates on high-risk jurisdictions.	FinCEN Advisories

USA Regulatory Guidelines an Directives

List/Guideline	Description	Source
Bank Secrecy Act (BSA)	The primary U.S. AML/CTF legislation requiring financial institutions to assist U.S. government agencies.	FinCEN - Bank Secrecy Act
USA PATRIOT Act	Expanded AML/CTF requirements for financial institutions, including customer identification programs.	USA PATRIOT Act Text
Office of Foreign Assets Control (OFAC) Regulations	Regulations enforcing economic and trade sanctions based on U.S. foreign policy and national security goals.	OFAC Regulations
Federal Financial Institutions Examination Council (FFIEC) BSA/AML Manual	Comprehensive guidance on AML/CTF compliance for U.S. financial institutions.	FFIEC BSA/AML Manual
National Risk Assessment of Money Laundering and Terrorist Financing	Government assessment identifying domestic high-risk areas.	U.S. National Money Laundering Risk Assessment

Financial Institutions Onboarding Requirements
☐ Evidence of Permission to carry out regulated activity (regulatory license) ☐ Completed Financial institutions due diligence questionnaire ☐ Application Form ☐ Signed Board Resolution authorising the account stating purpose and listing the account signatories/mandate ☐ Copy of policies and procedure ☐ Walk through of Client Onboarding and transaction monitoring procedure ☐ Certificate of Incorporation with details of shareholders and directors and any name change certificates (if applicable) ☐ Articles of Association ☐ Confirmation Statement (Shareholder and Director registers) ☐ Most recent Annual Accounts (audited if available) ☐ Proof of trading address if it differs from registered address (bank statement/utility bill) ☐ Proof of identity and address for all beneficial owners with 25% or more interest (Threshold can be reduced to ensure we have 75% of the beneficial ownership.
☐ Proof of identity and address for two Directors ☐ Proof of identity and address for authorised signatories/traders ☐ Evidence of nature of business (e.g. website) ☐ Confirmation of ownership structure from an independent and reliable source such as companies' registry, professional sources and open sources.

Counterparties Requirements
▯ Evidence of Permission to carry out regulated activity (regulatory license) – May be found from regulator website ▯ Completed Financial institutions due diligence questionnaire – (This is the only document they have to complete). ▯ Copy of policies and procedure – Some of the policies may be found from website ▯ Evidence of nature of business (e.g. website) ▯ Confirmation of ownership structure from an independent and reliable source such as companies' registry, professional sources and open sources.

Prohibited Jurisdictions
▯ Afghanistan ▯ Angola ▯ Belarus ▯ Bosnia-Herzegovina ▯ Burundi ▯ Central African Republic ▯ Congo, the Democratic Republic ▯ Cuba ▯ Ethiopia ▯ Guinea Bissau ▯ Guatemala ▯ Iran, Islamic Republic of ▯ Iraq ▯ Korea (the Democratic People's Republic of) ▯ Kosovo ▯ Lebanon ▯ Liberia ▯ Libya ▯ Mali ▯ Myanmar ▯ Nagorno-Karabakh ▯ Nicaragua ▯ Northern Cyprus ▯ North Korea ▯ Russian Federation ▯ Sahrawi Arab Democratic Republic ▯ Somalia

- South Ossetia
- South Sudan
- Sudan
- Syrian Arab Republic
- Tunisia
- Turkey
- Venezuela
- Yemen
- Zimbabwe
- Western Sahara
- Ukraine regions: Luhansk, Donetsk, Crimea and other occupied regions

High-Risk Jurisdictions

- Albania
- American Samoa
- Anguilla
- Antigua and Barbuda
- Aruba
- Azores (Portugal territory)
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belize
- Bermuda
- Botswana
- British Virgin Islands
- Brunei Darussalam
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Cayman Islands
- Central African Republic

- Chad
- Chile
- China
- Colombia
- Comoros
- Congo (Brazzaville)
- Cook Islands
- Costa Rica
- Croatia
- Curacao
- Djibouti
- Dominica
- Egypt
- Equatorial Guinea
- Eritrea
- Fiji
- French Polynesia
- Gaza Strip
- Gibraltar
- Guernsey
- Haiti
- Honduras
- Hong Kong
- India
- Isle Of Man
- Israel
- Jamaica
- Jersey
- Jordan
- Kenya
- Kyrgyzstan
- Madagascar
- Malaysia
- Maldives
- Marshall Islands
- Mauritania
- Mauritius
- Montserrat
- Morocco
- Mozambique
- Namibia
- Nauru
- Niger

- Nigeria
- Niue
- North Macedonia
- Pakistan
- Palau
- Panama
- Philippines
- Qatar
- Saint Helena, Ascension and Tristan da Cunha
- Saint Martin (French part)
- Saint Pierre and Miquelon
- Samoa
- Senegal
- Seychelles
- Solomon Islands
- South Africa
- St Kitts & Nevis
- Tajikistan
- Tanzania
- Thailand
- Tonga
- Trinidad & Tobago
- Turkmenistan
- Turks & Caicos
- Uganda
- United Arab Emirates
- United States Virgin Islands
- Uruguay
- Uzbekistan
- Vanuatu
- Vietnam
- West Bank (Palestinian Territory, Occupied)

Unsupported Industries

- Shell Banks
- Anonymous Shell Companies
- Businesses involved in the illegal drug trade
- Unlicensed gambling and gaming services
- Unlicensed money services businesses (MSBs)
- Dealers in arms and weapons
- Businesses involved in human trafficking or exploitation

- Prostitution and escort services
- Ponzi schemes and other pyramid sales schemes
- Businesses involved in the production or distribution of pornography
- Unregistered charities and non-profit organizations
- Businesses involved in the sale of counterfeit goods
- Unlicensed foreign exchange trading platforms
- Any business or activity that involves the exploitation of children
- Cryptocurrency mixing services or tumblers
- Businesses dealing in stolen goods
- Any other business or activity deemed illegal by regulatory authorities

SIGNATORY PAGE

Policy amended by: Igor Lavrih, CEO

Signature: _____

Place: Ljubljana, Slovenia

Date: 02.10.2025

Policy signed by: Igor Lavrih, CEO

Signature: _____

Place: Ljubljana, Slovenia

Date: 02.10.2025