AML/CTF Compliance Program

of
Hedgehog Solutions s.r.o.

Hedgehog Solutions s.r.o.

registration number 176 62 605
Vašátkova 1009/22, Černý Most, 198 00 Praha 9, Czech Republic

Hedgehog Solutions s.r.o. maintains full cooperation with law and regulatory authorities in legislations, investigations and inquiries.

This AML/CTF Compliance Program is a subject to an annual review.

Hedgehog Solutions s.r.o. adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

The company adopts a risk-based approach in the design and implementation of the AML/CTF Policy with a view to managing and mitigating ML/TF risks.

Hedgehog Solutions s.r.o. 6 Key AML/CTF Principles:

- to comply with AML/CTF legislation in the countries in which it operates;
- to strive to fulfil international standards as detailed by the Financial Action Task Force (FATF) recommendations;
- to work in conjunction with the governments of the countries Hedgehog Solutions s.r.o. operates in, as well as support their objectives in relation to the prevention, detection and control of ML/TF;
- Hedgehog Solutions s.r.o. may decide not to provide products or services based upon decisions guided by ML/TF risk appetite and corporate social responsibility;
- to comply with primary legislation on AML/CTF;
- to comply with Act No. 253/2008 Coll., on selected measures against the legitimisation of the proceeds of crime and financing of terrorism.

Hedgehog Solutions s.r.o. AML/CTF Compliance Program:

- forms part of its wider compliance regime, and is designed to meet the requirements of its legislative environment;
- ensures that Hedgehog Solutions s.r.o. is able to detect suspicious activities associated with money laundering, fraud, and terrorist financing, and report them to the appropriate authorities;
- focuses not only on the effectiveness of internal systems and controls developed to detect money laundering, but on the risk posed by the activities of customers with which Hedgehog Solutions s.r.o. does business;
- is built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organisation.

Prevention of Money Laundering & Terrorist Financing

The term *"money laundering" (ML)* means an act intended to have the effect of making any property:

(a) that is the proceeds obtained from the commission of an indictable offence or of any conduct which would constitute an indictable offence; or

(b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.

There are three common stages in the laundering of money, and they frequently involve numerous transactions. These stages are:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities;

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

The term *"terrorist financing" (TF)* means:

(a) the provision or collection, by any means, directly or indirectly, of any property –

(i) with the intention that the property be used; or

(ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used);

(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

FATF defines *"proliferation of weapons of mass destruction"* as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials.

The Financial Action Task Force (the FATF) is an inter-governmental body formed in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standard for combating of ML, TF and PF. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level,

the FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high-risk and other monitored jurisdictions which

could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large.

Hedgehog Solutions s.r.o. has established its AML/CTF Compliance Program to ensure that any money laundering risks identified by Hedgehog Solutions s.r.o. are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the company being used to facilitate any financial crimes. This program is designed to represent the basic standards of Anti-Money Laundering and Combating Terrorism Financing procedures and standards, which will be strictly observed by Hedgehog Solutions s.r.o..

The AML/CTF Compliance Program is based upon applicable AML/CTF laws and regulations. This program is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation. It also follows the AML principles of the Wolfsberg Group.

AML / CTF SYSTEMS

Hedgehog Solutions s.r.o. firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The company is, therefore, committed to the highest standards of Money Laundering and Combating Terrorism financing (AML/CTF) measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

Effective Controls

To ensure proper implementation of AML/CTF procedures and controls, Hedgehog Solutions s.r.o. has effective controls covering:

- Effective AML/CTF compliance program;
- Senior management oversight;
- Appointment of Compliance Officer / Money Laundering Reporting Officer (MLRO);
- Compliance and audit function;
- Staff screening and training.

The Director of Hedgehog Solutions s.r.o. is responsible for managing the business effectively and for the oversight of internal AML/CTF controls and systems. Director appoints the Compliance Officer/MLRO who has overall responsibility for the establishment and maintenance of Hedgehog Solutions s.r.o.' AML/CTF systems.

Three Lines of Defence

Hedgehog Solutions s.r.o. follows the three lines of defense framework when managing ML/TF risks. The three lines of defense is an industry model for managing risk. It is used to structure roles, responsibilities and accountabilities for decision making, risk and control management, and independent assurance. The three lines of defense are used as the fundamental guiding principle when performing the AML/CTF review.

Audit Function

Audit function shall be established to perform regularly reviews of the AML/CTF systems, e.g. sample testing, to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of Hedgehog Solutions s.r.o. business. Where appropriate, Hedgehog Solutions s.r.o. will seek a review from external auditors.

Independent Audit Functions include:

- Compliance and audit functions are independent in practice;
- The regular review is performed at a frequency of once a year;
- External party is leveraged to perform the auditing;
- Availability of direct communication to senior management through regular committees (compliance committee) or other means of direct communication.

Know Your Employee

The best way to reduce insider abuse is to stop it before it starts. It starts during the hiring process, with Hedgehog Solutions s.r.o. exercising the same precautions as it does when opening an account. Hedgehog Solutions s.r.o. performs due diligence on employees verifying any information supplied.

Integrity of Staff

Integrity is one of the fundamental values that Hedgehog Solutions s.r.o. seeks in the employees it is going to hire. Integrity involves moral judgment and character, honesty and leadership values.

Counter-Checking of Work Completed by Staff

Hedgehog Solutions s.r.o. performs occasional spot checks on work done by staff at all levels. Usually, these checks are undertaken by senior management to ensure that Hedgehog Solutions s.r.o. policies and procedures are being followed and everything is in the correct order.

Hedgehog Solutions s.r.o. has a “Zero Tolerance” policy regarding intentional violation of applicable laws prohibiting money laundering, terrorist financing and related financial crimes. Hedgehog Solutions s.r.o. will require the immediate discharge of an employee who commits such violations, and will refer such cases to the appropriate regulatory bodies.

Procedures for Employees engaged in a Suspicious Activity

If an employee is suspected of engaging in any type of unusual or questionable activity, this must be brought to the attention of both Senior Management and the Compliance officer immediately.

Senior Management and/or the Compliance officer will jointly investigate the actions of the employee in the most discreet manner. All actions taken to conduct the investigation must be documented.

Senior Management determines that the employee’s activity was prejudicial to the interests of the Company, it will determine whether disciplinary action is necessary. Senior Management may seek advice from legal counsel in such action.

In order to know its employees Hedgehog Solutions s.r.o. conducts:

- a criminal conviction search in jurisdictions where it is possible;

- credit checks;
- a private investigation, if thought necessary;
- an internet check before they are hired.

AML/CTF Training

Hedgehog Solutions s.r.o. has a clear policy towards staff training with respect to AML/CTF issues. Staff is being made aware of:

- Hedgehog Solutions s.r.o. and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROP, the OSCO and the UNATMO;
- any other statutory and regulatory obligations that concern Hedgehog Solutions s.r.o. and themselves under the DTROP, the OSCO, the UNATMO, and the possible consequences of breaches of these obligations;
- the Hedgehog Solutions s.r.o.' policies and procedures relating to AML/CTF;
- any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in Hedgehog Solutions s.r.o. with respect to AML/CTF.

The training is assigned for all groups of Hedgehog Solutions s.r.o.' staff:

- all new staff, irrespective of seniority;
- to the Compliance Officer/ MLRO;
- back-office staff, depending on their roles;
- managerial staff.

Training program provides staff with an understanding of the process of money laundering, the laws and regulations that make it illegal, and the responsibilities of employees to help detect and prevent it. The training on AML/CTF issues raises awareness of financial crime risks, global laws and regulations, laws and regulations applicable to Hedgehog Solutions s.r.o.

Annual AML Seminar

Designed for all operational staff and includes:

- General information: the background and history pertaining to money laundering controls, what money laundering and terrorist financing is;
- Legal framework: how AML/CFT laws and regulations apply to Hedgehog Solutions s.r.o. and its employees;
- Penalties for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment;
- How to react when faced with a suspicious client or activity;
- Internal policies, such as customer identification and verification procedures and CDD policies;
- What the legal record keeping requirements are;
- Duties and accountability of employees.

Ad-hoc Training

Provided regularly to all employees based on, but not limited to, changes in government regulations, changes/amendments in Hedgehog Solutions s.r.o.'s AML/CFT policies and procedures.

Hedgehog Solutions s.r.o. uses mix of training techniques and tools in delivering training, depending on the available resources and learning needs of its staff. These techniques and tools include visiting external seminars of Mastercard academy, on-line learning systems, focused classroom training, relevant videos as well as paper- or intranet-based procedures manuals. Hedgehog Solutions s.r.o. also includes available FATF papers and typologies as part of its the training materials. All materials are kept up-to-date and in line with current requirements and standards. The effectiveness of training is being monitored by testing the staff's understanding of AML/CTF issues and its ability to recognise suspicious activity. To achieve this Hedgehog Solutions s.r.o.'s Compliance Department conducts random testing sessions on a quarterly basis.

All training related records and documents are kept throughout the employment relationship with the employee and for a period of at least five years after the end of the employment.

RISK-BASED APPROACH (RBA)

By adopting a risk-based approach, financial institutions are able to ensure that measures to prevent or mitigate money laundering and financing threats are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

The inherent risk is assessed in course of identification of the specific products, services, customers, entities, and geographic locations. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered.

Risk assessment on the stage of on-boarding of a new customer is an opportunity for the management of Hedgehog Solutions s.r.o. to gain an insight into the type and nature of its potential customers, their geographic locations and business activities.

Verifying identities, making sure they're real, confirming they're not on any prohibited lists, and assessing their risk factors—ensures that Hedgehog Solutions s.r.o. keeps money laundering, terrorism financing, and more run-of-the-mill fraud schemes at bay.

Hedgehog Solutions s.r.o. determines the extent of its CDD measures and ongoing monitoring, using a risk-based approach (RBA) depending upon the background of the customer and the product, transaction or service used by that customer, so that preventive or mitigating measures are commensurate to the risks identified.

The RBA enables Hedgehog Solutions s.r.o. to subject its customers to proportionate controls and oversight by determining:

- the extent of the due diligence to be performed on the direct customer;
- the extent of the measures to be undertaken to verify the identity of any beneficial owner and any person purporting to act on behalf of the customer;
- the level of ongoing monitoring to be applied to the relationship;

- measures to mitigate any risks identified.

An RBA involves identifying and categorising ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An RBA does not refrain Hedgehog Solutions s.r.o. from engaging in transactions with customers or establishing business relationships with potential customers, but rather it assists Hedgehog Solutions s.r.o. to effectively manage potential ML/TF risks.

Non-acceptable Customers

Hedgehog Solutions s.r.o. does not accept clients from the industries as stated below:

- Trade /production/mediation in the trade of weapons;
- Trade of antiques works of art, numismatic values;
- Trade of ferrous, non-ferrous and rare metals and their wares, precocious stones;
- Production/recycling of explosive and nuclear fuel;
- Unregulated charities and other unregulated organisations;
- Dealers of high-value precious goods;
- Adult industries;
- Wholesale trade of alcohol and tobacco products;
- Unlicensed financial institutions / money service businesses.

The detailed information on prohibited business types is captured in *Appendix* hereto.

Prohibition of Anonymous Accounts

Hedgehog Solutions s.r.o. does not maintain anonymous accounts or accounts in fictitious names for any new or existing customer.

Prohibition of Shell Banks

Hedgehog Solutions s.r.o. does not maintain correspondent relationships with shell banks, which are defined as non-resident banks that have no permanent executive bodies in the countries in which they have been registered, and has not entered into correspondent relationships with banks that allow their accounts to be used by shell banks.

Customer Due Diligence

Customer due diligence (CDD) is central to an effective anti-money laundering and counter-terrorism financing (AML/CTF) regime. Hedgehog Solutions s.r.o. takes measures to identify and verify each of its customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.

CUSTOMER DUE DILIGENCE (CDD)

Identification and Verification of the Customer's Identity

Hedgehog Solutions s.r.o. applies the following CDD measures:

- identification of the customer and verification of the customer's identity using reliable, independent source documents, data or information;

- identification and taking reasonable measures to verify the beneficial owner's identity so that Hedgehog Solutions s.r.o. is satisfied that it knows who the beneficial owner is, including in the case of a legal person or trust, measures to enable Hedgehog Solutions s.r.o. to understand the ownership and control structure of the legal person or trust;

- obtaining an information on the purpose and intended nature of the business relationship unless the purpose and intended nature are obvious;

If a person purports to act on behalf of the customer, Hedgehog Solutions s.r.o. take s measures to: identify the person and take reasonable measures to verify the person's

- identity using reliable and independent source documents, data or information;
- verify the person's authority to act on behalf of the customer.

CDD requirements should apply:

- at the outset of a business relationship;
- before performing any occasional transaction;
- when Hedgehog Solutions s.r.o. suspects that the customer or the customer's account is involved in ML/TF irrespective of the amount of transaction;
- when Hedgehog Solutions s.r.o. doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

Identification and Verification of a Beneficial Owner

A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. Hedgehog Solutions s.r.o. verifies the identity of beneficial owner(s) owning or controlling 25% or more of the voting rights or shares of the legal entity, taking reasonable measures based on ML/ TF risks, so that Hedgehog Solutions s.r.o. knows who the beneficial owner(s) is.

When an individual is identified as a beneficial owner, Hedgehog Solutions s.r.o. obtains the following identification information:

- full name
- date of birth
- nationality
- identity document type and number

Hedgehog Solutions s.r.o. obtains the residential address (and permanent address if different) of the beneficial owners and adopts a risk-based approach to determine the need to verify the address, taking in account the number of beneficial owners, the nature and distribution of the interests in the entity and the nature and extent of any business, contractual or family relationship.

Identification and Verification of a Person who Purports to Act on Behalf of the Customer

If a person purports to act on behalf of the customer, Hedgehog Solutions s.r.o.:

- identifies the person and takes reasonable measures to verify the person's identity on the basis of documents, data or information provided by:
  i) a governmental body;
  ii) the relevant authority or any other relevant authority;
  iii) any other reliable and independent source that is recognised by the relevant authority; and
- verifies the person's authority to act on behalf of the customer.

In general, Hedgehog Solutions s.r.o. identifies and verifies the identity of those authorized to give instructions for the movement of funds or assets.

Hedgehog Solutions s.r.o. obtains written authority in order to verify that the individual purporting to represent the customer is authorised to do so.

Purpose and Intended Nature of Business Relationship

Unless the purpose and intended nature are obvious, Hedgehog Solutions s.r.o. obtains satisfactory information from all new customers as to the intended purpose and reason for opening the account or establishing the business relationship, and records the information on the account opening documentation.

Depending on the Hedgehog Solutions s.r.o. risk assessment of the situation, information required may include:

- nature and details of the business/occupation/employment;
- the anticipated level and nature of the activity that is to be undertaken through the relationship (e.g. what the typical transactions are likely to be);
- location of customer;
- the expected source and origin of the funds to be used in the relationship;
- initial and ongoing source(s) of wealth or income.

Keeping Customer's Information Up-to-Date

Hedgehog Solutions s.r.o. takes steps from time to time to ensure that the customer information that has been obtained is up- to-date and relevant. To achieve this, Hedgehog Solutions s.r.o. undertakes periodic reviews of existing records of customers.

An appropriate time to do so is upon certain trigger events such as:

- when a significant transaction (not only of a big amount, but also unusual) is to take place;
- when a material change occurs in the way the customer's account is operated;
- when the customer's documentation standards change substantially;
- when Hedgehog Solutions s.r.o. is aware that it lacks sufficient information about the customer concerned.

KNOW YOUR CUSTOMER / CUSTOMER ON-BOARDING

Identification and verification of natural persons

Hedgehog Solutions s.r.o. requests identity document (Passport or ID Card), specifying:

• full name
• date of birth
• nationality
• identity document type and number.

Address identification and verification

Hedgehog Solutions s.r.o. verifies the residential address (and permanent address if different) of a direct customer with whom it establishes a business relationship.

Methods for verifying residential addresses may include obtaining:

- a recent utility bill issued within the last 3 months;
- recent correspondence from a Government department or agency (i.e. issued within the last 3 months);
- a statement, issued by an authorized institution, a licensed corporation or an authorized insurer within the last 3 months.

Identification of a Legal Entity

With respect to legal entities, Hedgehog Solutions s.r.o. pays special attention when looking behind the customer to identity those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets. Verifying the identity of the beneficial owner(s) is being carried out using reasonable measures based on a risk-based approach. For a customer other than a natural person, Hedgehog Solutions s.r.o. ensures that it fully understands the customer's legal form, structure and ownership, and additionally obtains information on the nature of its business, and the reasons for seeking the product or service unless the reasons are obvious.

Hedgehog Solutions s.r.o. conducts reviews from time to time to ensure the customer information held is up-to-date and relevant; methods by which a review could be conducted include conducting company searches, seeking copies of resolutions appointing directors, noting the resignation of directors, or by other appropriate means.

Hedgehog Solutions s.r.o. obtains and verifies the following information in relation to a customer which is a legal entity:

- full name
- date and place of incorporation
- registration or incorporation number
- registered office address in the place of incorporation
- web-site requirements:

i) Cross-reference of the web-site and the Company (Merchant's web-site as well as their Terms & Conditions (Merchant Agreement) are to contain the following information about the Company: address, register number, license (if applicable);

ii) Terms & Conditions (MerchantAgreement);

iii) Payment & Refund Policy;

iv) Privacy Policy.

If the business address of the customer is different from the registered office address in the place of incorporation, Hedgehog Solutions s.r.o. obtains information on the business address and verifies it.

In the course of verifying the customer's identity, Hedgehog Solutions s.r.o. obtains the following data and documents:

- a copy of the certificate of incorporation and business registration (where applicable);
- a copy of the company's memorandum and articles of association which evidence the powers that regulate and bind the company;
- details of the ownership and structure control of the company, e.g. an ownership chart;
- the names of all directors.

Hedgehog Solutions s.r.o. shall also:

- confirm the company is still registered and has not been dissolved, wound up, suspended or struck off;
- independently identify and verify the names of the directors and shareholders recorded in the company registry in the place of incorporation;
- verifiy the company's registered office address in the place of incorporation.

Beneficial Owners

Hedgehog Solutions s.r.o. identifies and records the identity of all beneficial owners, and takes reasonable measures to verify the identity of:

- all shareholders holding 25% of the voting rights or share capital (the threshold shall be lowered to 10% for each high-risk relationship);
- any individual who exercises ultimate control over the management of the corporation;
- any person on whose behalf the customer is acting.

For companies with multiple layers in their ownership structures, Hedgehog Solutions s.r.o. takes measures to ensure that it has an understanding of the ownership and control structure of the company.

ENHANCED CUSTOMER DUE DILIGENCE (EDD)

Hedgehog Solutions s.r.o. applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high risk situation generally occurs where there is an

increased opportunity from money laundering or terrorist financing through the service and product Hedgehog Solutions s.r.o. provides or from a customer of Hedgehog Solutions s.r.o..

What the enhanced due diligence actually entails will be dependent on the nature and severity of the risk.

High-Risk Situations

In any situation that by its nature presents a higher risk of ML/TF, Hedgehog Solutions s.r.o. takes additional measures to mitigate the risk of ML/TF.

Additional measures or EDD may include:

- obtaining additional information on the customer (e.g. connected parties, accounts or relationships) and updating more regularly the customer profile including the identification data;
- obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity), the source of wealth and source of funds;
- obtaining the approval of senior management to commence or continue the relationship; and
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

Politically Exposed Persons (PEPs)

Politically Exposed Persons:

- an individual who is or has been entrusted with a prominent public function and includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
- a spouse, a partner, a child or a parent of an individual falling within paragraph above, or a spouse or a partner of a child of such an individual;
- a close associate of an individual falling within paragraph above.

A PEP's close associate is:

- an individual who has close business relations with a person falling under the definition of PEP, including an individual who is a beneficial owner of a legal person or trust;
- an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under the definition of PEP.

In order to reduce possible risks Hedgehog Solutions s.r.o. conducts EDD at the outset of the business relationship and ongoing monitoring where it knows or suspects that it has business relationship with a PEP.

For that purpose Hedgehog Solutions s.r.o.:

- makes reference to publicly available information;
- screens against commercially available databases for determining whether a customer or a beneficial owner of a customer is a PEP;

- uses publicly available information or refer to relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations to assess which countries are most vulnerable to corruption.

In relation to PEPs, Hedgehog Solutions s.r.o. applies the following EDD measures:

- obtaining approval from Hedgehog Solutions s.r.o.' senior management;
- taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds;
- applying enhanced monitoring to the relationship in accordance with the assessed risks.

Source of Wealth vs Source of Funds

Establishing the customer's source of wealth or source of funds is a core requirement of EDD.

Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although Hedgehog Solutions s.r.o. may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and Hedgehog Solutions s.r.o. (e.g. the amounts being invested, deposited, or wired as part of the business relationship). Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

Hedgehog Solutions s.r.o. collects information relating to the source of wealth or source of funds of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.

The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to Hedgehog Solutions s.r.o..

The following documents, data, or information could be considered reliable and independent:

- government-issued or registered documents or data;
- full bank and other investment statements;
- full payslip or wage slip or other documents confirming salary;
- inheritance (stamped grant of probate, stamped grant of letters of administration);
- audited financial accounts from a chartered accountant or Charities Services;
- letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer;
- a copy of a will;
- sales and purchase agreements.

High-risk jurisdictions

- Countries-subject to OFAC sanctions;

- Countries identified as supporting international terrorism;
- Jurisdictions, determined to be of primary money laundering concern and subject to special measures;
- Offshore financial centres;
- Jurisdictions with deficiencies in combating money laundering and terrorist financing identified by FATF.

Hedgehog Solutions s.r.o. gives particular attention to, and exercises extra care in respect of:

- business relationships and transactions with persons (including legal persons and other financial institutions) from or in jurisdictions that do not or insufficiently apply the FATF Recommendations;
- transactions and business connected with jurisdictions assessed as higher risk.

The Financial Action Task Force ("FATF") has published a list of countries/jurisdictions classified as being "non-cooperative in the international fight against money laundering". The list may be modified and updated as needed. The FATF list is kept current by the Compliance officer/MLRO.

In addition to ascertaining and documenting the business rationale for establishing a relationship, Hedgehog Solutions s.r.o. takes reasonable measures to establish the source of funds of such customers.

In determining which jurisdictions do not apply, or insufficiently apply the FATF Recommendations, or may otherwise pose a higher risk, Hedgehog Solutions s.r.o. considers, among other things:

- circulars issued by relevant authorities;
- whether the jurisdiction is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN);
- whether the jurisdiction is identified by credible sources as lacking appropriate AML/CTF laws, regulations and other measures;
- whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organisations operating within it;
- whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra- national or international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organisations. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

Hedgehog Solutions s.r.o. will make a reference to publicly available information or relevant reports and data bases on corruption risk, e.g. Transparency International Corruption Perceptions Index.

SANCTIONS POLICIES

With a view to ensure that there are no payments to or from a person on a sanctions list issued by an overseas jurisdiction, Hedgehog Solutions s.r.o. conducts screening against lists of FATF not-compliant countries, in addition to the lists of sanctioned countries, entities and persons.

Hedgehog Solutions s.r.o. takes measures to thoroughly screen its customers and gather as much information as possible about them and their accounts. This helps to ensure that the customers are not involved in financial crimes.

Many transactions that are completed in order to send money to terrorist organisations are small and innocuous. Terrorist financiers purposefully do not send large amounts of money at once, as they wish to avoid the attention of both governments and financial institutions. Additionally, individuals who finance terrorism also use trade-based money laundering schemes in order to get their money across borders. This is becoming much more common, and it is a difficult problem to track down.

Hedgehog Solutions s.r.o. takes measures to ensure compliance with the relevant regulations and legislation on terrorist financing. It is particularly vital that Hedgehog Solutions s.r.o. is able to identify and report transactions with terrorist suspects and designated parties.

Hedgehog Solutions s.r.o. maintains a database of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have been made known to it. Alternatively, Hedgehog Solutions s.r.o. makes arrangements to access to such a database maintained by third party service providers.

Hedgehog Solutions s.r.o. screens customers and transactions against following lists:

- Consolidated United Nations Security Council Sanctions List
- OFAC Specially Designated Nationals And Blocked Persons List (SDN)
- Other OFAC sanctions lists
- EEAS-consolidated list of persons, groups and entities subject to EU financial sanctions.

To avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties, Hedgehog Solutions s.r.o. implements an effective screening mechanism, which includes:

- screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship;
- screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable;
- screening all relevant parties in a cross-border wire transfer against current database before executing the transfer.

UNATMO is an ordinance to further implement a decision under UNSCR 1373 (2001) relating to measures for prevention of terrorist acts and a decision under UNSCR 2178 (2014) relating to the prevention of travel for the purpose of terrorist acts or terrorist training; as well as to implement certain terrorism-related multilateral conventions and certain FATF Recommendations. All UN member states are required to freeze any funds, or other financial assets, or economic resources of any person(s) named in these lists and to report any suspected name matches to the relevant authorities.

Where a person or property is designated by a Committee of the UNSC as a terrorist/terrorist associate or terrorist property respectively, the Chief Executive may publish a notice in the Gazette specifying the name of the person or the property. Besides, the Chief Executive may make an application to the Court of First Instance for an order to specify a person or property as a terrorist/terrorist associate or terrorist property respectively, and if the order is made, it will also be published in the Gazette.

A number of provisions in the UNATMO are of particular relevance to Hedgehog Solutions s.r.o., and are listed below:

- section 6 empowers the Secretary for Security (S for S) to freeze suspected terrorist property;
- section 7 prohibits the provision or collection of property for use to commit terrorist acts;
- section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates;
- section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate;
- section 11L prohibits any person from providing or collecting any property to finance the travel of a person between states with the intention or knowing that the travel will be for a specified purpose, i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training).

Hedgehog Solutions s.r.o., operating internationally, is aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect its operations, Hedgehog Solutions s.r.o. considers what implications exist for its procedures and takes appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable.

OFAC Compliance

It is the policy of Hedgehog Solutions s.r.o. to comply with all OFAC requirements and directives that restrict providing services, conducting business with, maintaining accounts for, or handling transactions or monetary transfers for foreign countries or foreign nationals listed on the Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals (SDNs) and Blocked Entities.

Hedgehog Solutions s.r.o. shall not open a relationship for, handle a transaction or monetary transfer for, or do business with any person, government or other entity on the OFAC list of Specially Designated Nationals and Blocked Entities. Through screening and monitoring, the Company will identify such customers or transactions, and if it is found, contact OFAC immediately and all directives as to rejecting, restricting, blocking or seizing will be followed.

As per new relationship opening procedure, no new relationship will be established without passing through the steps indicated and obtain the necessary approvals. As part of the relationship opening procedure, the Compliance Department will check the names of all, business owners, and authorized signers against OFAC's master list of "Specially Designated Nationals and Blocked Persons" (SDN list), and check the prospective customer's geographical location for embargoed countries and cities by putting the information through the system prior to opening the relationship.

The system will check names against the OFAC list and prior to approving the relationship. The system checks the entered name for matching spelling, close matches, name variations and phonetically. If the name of the prospective customer is a match or possible match to a name in the OFAC list, the system will displays the potential match, and maintain an electronic record of such a match to be included in the documentation.

The Company's staff is trained to recognize false positive matches and can continue with the transaction in the event a false positive match is displayed. The system will prompt the Compliance Staff to document the reason for the false positive, and will maintain that record in an electronic file.

Any close matches that cannot be easily categorized as a false positive must be immediately brought to the attention of the Compliance Officer for validation.

Appendix. Prohibited Business Types

General business Services	Description of prohibited activity Types
Adult Content	Any merchant connected with visual content, such as Pomography or violence, that is not generally thought to be a appropriate for viewing by children
Alcohol sales via internet	Merchants selling alcohol products via the internet, even if the sale of those items is NOT restricted to the merchant own country of domicile.
Chemicals and Allied Products	Wholesale distributors of chemicals and lied products not elsewhere classified. Products for sale are typically used for industrial purposes. Examples include industrial acids, ammonia and alcohol, heavy, aromatic and other chemicals, chlorine, compressed and liquefied gases, detergents, fuel and oil additives, resins, sats, turpentine, sealants, rust proofing chemicals, coal tar products, dry ice, dyestuffs, glue, gelatin, and explosives.

Child Pornography	Any merchant who provides products or services associated with actual or suggested child ponography. Includes. any merchant or website who uses the following terminology to promote their product: ‘olita’ ‘pedo’ ‘pre-teen’ or any other terminology that suggests child pornography.
Cigarette/electronic cigarette/Tobacco Vape sales	Any that sell cigarettes/electronic cigarette/tobacco vape via internet even if the scale of those items is NOT restricted to the merchants own country of domicile
Counterfeit goods	Merchants selling counterfeit merchandise (well-known brands) or goods where merchants are infringing on intellectual property rights of trade mark owners (including illegal use of games, game keys etc) д.)
Non-prescription drugs such as pharmaceutical wonder drugs e.g. Steroids, diet pills & all Internet drug stores	Outlets offering nonprescription drugs such as: pharmaceutical wonder drugs e.g. steroids, diets pills, and all Internet drug stores
Drug Paraphernalia	Any business whose products are solely intended for aiding the consumption of illegal drugs.
Fortune tellers	includes fortune-tellers, tarot card readers, and mystics.
Guns, firearms, munitions sale & distribution	Any- sale of firearms by any method

Financial and other Pyramid Sales	includes sales structures where multiple levels of sales people are making money off one another with no real product or a questionable product to sell: income of the first parties ants of pyramid is paid at the expense of new participants.
Sexual Encounter/Escort Firms	Any merchant connected with sexual encounter, including escort services, massage parlors, spas, etc., where sexual encounters are permitted.
Political Organizations and parties	Merchants representing the membership organizations that promote the interests of a national, state, or local political party or candidate, including political groups organized specifically to raise funds for a political party or individual candidate.
Religious Organizations (excluding nationally recognized religious organizations/faiths)	Religious organizations that provide worship services, re gious training or study, and religious activities, including collection of donations