Solve.Care Foundation OU

Anti-Money Laundering ("AML") and Counter-Terrorist Financing ("CTF") Policy: Compliance and Supervisory Procedures

Contents

1. The Company

Solve.Care Foundation OU ("Solve.Care") is a company incorporated and acting under the law of Estonia, having its registered office at Narva mnt 5, Tallinn city, Harju County, 10117, Estonia.

Solve.Care was established to revolutionize healthcare delivery, care coordination and benefits administration around the globe. Solve.Care operates an innovative online-platform, which consists of Care.Wallet, Care.Protocol, Care.Coin, Care.Card and several other components, that combines decentralization with synchronization to connect stakeholders with each other and redefine care, cost and convenience for everyone.

2. The purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing Policy: Compliance and Supervisory Procedures ("AML/CTF Policy") is to prohibit and actively prevent money laundering ("ML") and any activity that facilitates ML or the financing of terrorism (FT) or criminal activities by complying with all applicable requirements under the European and Estonian law and its implementing regulations.

Solve.Care puts reasonable efforts in place to control and to limit ML/FT risk, including dedicating the appropriate means.

Solve.Care is committed to high standards of anti-money laundering / counter the financing of terrorism (AML/CFT) compliance and requires management, employees and subsidiaries to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

The Solve.Care AML / CTF Policy is created to be compliant with:

- International standards: recommendations and papers from the Financial Action Task Force ("FATF") etc.;
- European laws and regulations related to AML/CFT: 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 etc.;
- Estonian laws and regulations related to AML/CFT: Money Laundering and Terrorist Financing Prevention Act as of 27.11.2017 and other regulations and guidelines.

Our AML/CTF Policy, procedures and internal controls are designed to ensure compliance with the above said regulations, recommendations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

3. Definition of Money Laundering and Terrorism Financing

Money Laundering means:

a. the conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the

property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

b. the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;

c. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

d. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money laundering shall be regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.

Knowledge, intent or purpose required as an element of the activities referred to in this section 3 may be inferred from objective facts.

Money laundering shall be regarded as such also where the details of a criminal activity which generated the property to be laundered have not been identified.

Terrorism financing means:

the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

4. AML/CFT compliance function

4.1. Corporate organization

In accordance with the AML/CFT legislation, Solve.Care has appointed a responsible at the "highest level" among its Board of Directors for the prevention of ML/FT: the CEO at Group level.

Moreover, an Anti-Money Laundering and Counter-Terrorist Financing Compliance Officer ("AML Compliance Officer") is in charge of the enforcement of this AML/CFT Policy and procedures within the Solve.Care.

AML is placed under the direct responsibility of the AML Compliance Officer, himself under the direct responsibility of the Chief Executive Officer.

The duties of the AML Compliance Officer include monitoring the Solve.Care's compliance with AML/CFT obligations, overseeing communication and training for employees, and other duties Solve.Care will assign to the AML Compliance Officer. The AML Compliance Officer also ensures that Solve.Care keeps and maintains all of the required AML records and will ensure that suspicious activity reports (SARs) are filed with the responsible authorities when appropriate. The AML Compliance Officer is vested with full responsibility and authority to enforce the Solve.Care's AML program.

4.2. AML/CFT Policy implementation requirements

Each major change of Solve.Care's AML/CFT policy is subject to approval by the company's Management Board.

4.3. Enterprise-wide risk assessment

We at Solve.Care understand the specifics and how unique is our business, therefore we are eager to comply with policies and guidelines applicable in full or in part to the similar kind of operations. Thus, we believe we should take a risk based approach to combating ML and TF. The risk assessment is a critical component of the Solve.Care AML/CFT compliance management program.

As part of the risk-based approach, Solve.Care has an AML Enterprise-Wide Risk Assessment Policy ("EWRA") to identify and understand risks specific to Solve.Care operations. The Solve.Care AML risk profile is determined after identifying and documenting the risks inherent to its business such as the products and services Solve.Care offers, the customers to whom such products and services are offered, transactions performed by these customers, delivery channels used, the geographic locations of Solve.Care's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML/CFT risk categories is based on Solve.Care understanding of regulatory requirements and industry guidance.

The EWRA is yearly reassessed.

5. Enterprise minimum standards

Solve.Care has established standards regarding Know-Your-Customer ("KYC"). These standards require due diligence for each prospective customer, mainly:

- Customer – a natural or legal person;
- Representative of the customer – an individual who is authorized to act on behalf of the customer;
- Beneficial Owner of the customer;
- Politically exposed person ("PEP") or a person connected with the PEP.

Solve.Care conducts due diligence before entering into a business relationship via identification and verification of customer's identity and, as the case may be, his representatives and beneficial owners on the basis of documents, data or information obtained from a reliable source compliant with the domestic and European AML/CFT legislation and regulation, which Solve.Care need to establish a portfolio of the user and access the risk, connected to it.

Interpretation of the KYC principle begins with identification of the customer by means of the necessary identification documents.

If the identification is completed by other information gathered, in this case the **Customer Acceptance Policy** to be applied.

In addition to these objective criteria, there are subjective elements which may arouse suspicions regarding a customer and to which particular attention should be paid.

Finally, as KYC does not involve static data, but dynamic data through the relationship with the customer, it also needs follow-up and ongoing monitoring of the customer.

5.1. Customer identification and verification (KYC)

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy.

Natural person needs to provide at least:

- first name, last name;
- date of birth, place of birth;
- home address;
- phone number and email;
- government issued ID document (both sides);
- proof of residence (utility bill or similar);
- other information and documents on the request of Solve.Care.

Only persons, who are older than 18 years old can be Solve.Care's customers.

Legal person needs to provide at least:

- business name of the legal person;
- registry code or registration number and the date of registration;
- proof of the registered office/seat;
- proof of representation;
- articles of association;
- other information and documents on the request of Solve.Care.

Accreditation documents

- Signed letter from a registered broker-dealer,
- an SEC-registered investment adviser,
- a licensed attorney or certified public accountant.
  Not older than 90 days.

The above listed documents will be recorded in a centralized system. Each person identified must be registered by IT means.

A person will not be accepted as a customer if the identification process proves to be incomplete.

Solve.Care makes sure to protect customer's personal data in accordance with the relevant laws and the Privacy Policy.

<u>The specific case of the due diligence exercised on the acceptance of politically exposed persons (PEP)</u>.

The currents legislation requires account to be taken of increased due diligence being extended to politically exposed persons who are Estonian residents. Concrete application at Solve.Care is reflected by a specific identification procedure for customers referenced as PEP, whatever their place of residence.

5.2. Risk Profile calculation

To assist in determining the level of AML/CFT due diligence to be exercised with regard to the customer, a "Compliance" risk profile is calculated first of all on entry into relations and is divided in three levels: Low, Medium, High:

a) **Low Risk**:
The risk level is low, there are no high risk characteristics present.

b) **Medium Risk**:
1) Customer is from high risk country;
2) Customer is a local PEP or a person associated with a PEP;
3) the legal person's area of activity is associated with enhanced money-laundering risk;
4) the legal person is situated in a country, which is listed in the list of risk countries;
5) the legal person's activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen;
6) the representative or the beneficial owner / shareholder of a legal person is a local PEP or his / her family member.

c) **High Risk**:
1) Customer is suspected to be or to have been linked with a financial offence or other suspicious activities.
2) Customer is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries.
3) the representative or the beneficial owner / shareholders of a legal person is a PEP or his or her family member;
4) there is information that legal person is suspected to be or to have been linked with a financial offence or other suspicious activities;
5) a legal person registered outside the European Economic Area, whose field of business is associated with a high risk of Money Laundering, or registered in a low tax rate country.

5.3. Risk categories

Risk by customers:

- *Suspicious facts such as but not limited to the*: discrepancies in provided ID documents, fictitious person, stolen identity, counterfeited id document, post box home address, pervious financial crime record, terrorist record, wanted person, no contact phone number, not valid documents, discrepancies in provided documents for the legal person, etc.

Politically exposed persons such as but not limited to the:

- *prominent public functions*: head of state, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials.

Risk by countries:

- *Country of residence / nationality is a country with prohibition/restriction on cryptocurrencies such as but not limited to*: Afghanistan, Algeria, American Samoa, Bangladesh, Bolivia, China, Democratic Republic Of Congo, Democratic People's Republic of Korea, Ecuador, Egypt, Ethiopia, Fyr Macedonia, India, Iran, Iraq, Kyrgyzstan, Pakistan, Palestine, Qatar, Saudi Arabia, Syria, Morocco, Nepal, United States of America, Vanuatu, Vietnam, Zambia.

- *Resident / Citizen of the high risk countries such as but not limited to*: Bahrain, Yemen, Jordan, Kuwait, Lebanon, Libya, Malaysia, Mali, Mauritania, Nigeria, Oman, Somalia, Serbia, Sri Lanka, Sudan, Tunisia, Turkey, Ethnic Groups Of Caucasus Belonging To Russian Federation (Chechens, Etc.), Trinidad & Tobago.

- *Low tax or tax-free countries such as but not limited to*: United Arab Emirates, Oman, Bahrain, Qatar, Saudi Arabia, Kuwait, Bermuda, Cayman Islands, The Bahamas, Brunei, Vanuatu, Anguilla, Belize, Costa Rica, Guatemala, Panamá, Nicaragua.

Risk by transactions:

- Solve.Care shall inspect any outstanding transaction, which include but is not limited to the: large transactions that do not correspond to user's source of funds and/or source of wealth etc.

5.4. Customer acceptance policy

Several elements require the establishment of a customer acceptance policy, in particular:

- accepting as customers only persons and entities with which Solve.Care may and wishes to develop commercial relations, and who correspond to the Solve.Care's current business model, ambitions and means;
- ensuring that the company has a good knowledge of the customer (KYC) and can exercise the due diligence appropriate to their level of risk from the start of the customer relations;
- avoiding Solve.Care entering into business relations with persons who might involve it in money laundering or terrorism financing transactions;
- meeting a legal / regulatory requirement;
- applying the risk-based approach run by Solve.Care in categorizing customers in relation to risk criteria.

Principles

The acceptance policy is applied to any person or entity asking for a transaction, product or service from Solve.Care.

Solve.Care will not accept customer relations with persons or entities not meeting this AML/CTF Policy and other documents mentioned herein, or whose legitimate intentions do not immediately appear to be sufficient, or included in the Estonian or European Union lists of persons or entities under financial sanction, or carrying on a commercial activity which is considered by Solve.Care as particularly at risk. Moreover, Solve.Care does not authorize anonymous transactions.

5.5. Ongoing customer due diligence

For some dedicated higher risk customer categories, a periodically risk-based review is carried out to ensure that customer-related data or information is kept up-to-date.

The current KYC review process regarding the other customer categories is essentially based on an "awareness principle" following the examination of a dedicated file by the AML team. This awareness principle consists in asking the authorized manager henceforth to closely perform a periodic KYC review of the customer.

5.6. Ongoing SOLVE wallet holders monitoring

In addition to the customer due diligence process, AML/CTF-Compliance ensures also that a SOLVE "wallet holders monitoring" is conducted to detect that the wallet holders related data or information is kept up-to-date. The "wallet holders monitoring" is periodically reviewed, but not less than once in the quarter and according to KYC standards.

5.7. Ongoing transaction monitoring

AML/CTF-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose.

Implemented internal controls will serve as ongoing monitoring system in order to detect the suspicious activity or transaction. When such suspicious activity is detected, Solve.Care shall determine whether a filing with any law enforcement authority is necessary. Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious and Solve.Care may wish to make a filing with a law enforcement authority, even if no money or CAN is lost as a result of the transaction.

Solve.Care shall initially make the decision of whether a transaction is potentially suspicious. Once Solve.Care's has finished the review of the transaction details, AML Compliance Officer will consult with its management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed. Solve.Care shall maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing.

5.8. Embargos and sanctions screening

To ensure compliance with the applicable sanctions against persons and entities, Solve.Care has put in place a list matching system in order to compare the names of its customers with official lists from Estonia, the European Union, the OFAC or the UN.

In addition to the above and in order to provide all business lines with up-to-date information related to jurisdictions under embargo, Solve.Care internally edits and maintains a **Country Watch-List** ("CWL") including the following jurisdictions which are:

- subject to the EU sanctions;
- subject to the US sanctions;
- designated by officials (like FATF) as subject to a higher money laundering risk;

- considered as a higher money laundering risk by Estonian authorities.

6. Organization of internal control

6.1. Suspicious transactions reporting

Solve.Care implements and maintains its internal procedures, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting, how to maintain records of the information used to verify a person's name, address and other identifying information are required under this Policy.

All and any reports of atypical transactions are analyzed within the AML team in accordance with the internal procedures. Depending on the result of this examination and on the basis of the information gathered, the AML team:

- will decide whether it is necessary or not to send a report to the Financial Intelligence Unit, in accordance with the legal obligations provided in the Money Laundering and Terrorist Financing Prevention Act as of 27.11.2017;
- will decide whether or not it is necessary to terminate the business relations with the customer.

6.2. Record keeping

The following are required steps in the record keeping process:

- Solve.Care shall maintain a record of identifying information provided by the customer.
- Where Solve.Care relies upon a document to verify identity, Solve.Care shall maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.
- Solve.Care shall also record the methods and result of any additional measures undertaken to verify the identity of the customer.
- Solve.Care shall record the resolution of any discrepancy in the identifying information obtained.

Records of data obtained for the purpose of identification will be kept for a minimum period of five years.

6.3. Training

Solve.Care has developed different ways of training and awareness in order to keep its staff aware of the AML/CFT duties. The training and awareness program is reflected in its usage by:

- a mandatory AML learning training program;
- academic AML learning sessions for all new branch employees.

Any training sessions are given by an AML-specialist working in Solve.Care' AML team.

6.4. Auditing

Internal audit regularly establishes missions and reports about AML/CFT activities.

7. Privacy considerations

Although suspicious activity reporting can be shared within the Solve.Care Group, there are certain privacy requirements that must be considered. Members of a Solve.Care Group should be conscious of the privacy implications when sharing any information between entities. This includes situations where a member of a Solve.Care Group that is based overseas, or a third-party provider, could be required to submit a suspicious transaction report or equivalent in that jurisdiction.

In accordance with the AML/CFT legislation, Solve.Care do its best efforts for protections of personal information by requiring all members of a Solve.Care Group, including overseas entities, to agree in writing to comply with privacy principles established by the EU and other applicable jurisdictions. The privacy requirements extend to the record-keeping obligations related to that personal information.

ANNEX A
GUIDELINES AND SCHEDULE OF AML/CFT AUDIT OF SOLVE WALLET HOLDERS

AML and CFT Compliance Checking Schedule

- AML officer is responsible for conducting periodic audit in accordance with industry best practices, available software and services, at reasonable cost to the company, per the following schedule
    - Q1 2019: Between March 1 and March 15, 2019
    - Q2 2019: Between June 1 and June 15, 2019
    - Q3 2019: Between September 1 and September 15, 2019
    - Q4 2019: Between December 1 and December 15, 2019

- Schedule for subsequent years should be published on or before December 15th of the prior year
    - By way of example, Schedule for 2020 should be published by December 15, 2019