AML/CTF POLICY

CBRO UAB IS regulated by the Lithuanian Financial Crime Investigation Service (FNTT.LT) that is operating under The Ministry of the Interior of the Republic of Lithuania.

The Rules are prepared in accordance with the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other applicable legal acts of the Republic of Lithuania.

The Rules describe how the Company will organize and ensure the adequate anti-money laundering and counter terrorism financing procedures. The implementation of the Rules will ensure that the name, reputation and financial integrity of the Company, whilst ensuring compliance with all necessary laws and regulations.

I. CUSTOMER IDENTIFICATION

The Company takes all necessary, proportionate measures to identify its customer and to verify the identity of the Customer and Customer's Beneficial Owners. The Company takes measures and determine identity of the Customer or his representative. Every new customer shall go through the KYC process according to the Rules. Their risk profile is classified as low, medium, or high risk for ML/TF based on criteria set out in the Rules.

CBRO UAB will verify:

1.1. Customer's identity;

1.2. Customer's residency (registration place, if Customer is a legal entity);

1.3. Nature of business activity;

1.4. Actual location of business activities;

1.5. Customer's (legal entity's) ownership and complexity of control structure;

1.6. Nationality of Beneficial Owner;

1.7. Volume and nature of transactions carried out by the Customer;

1.8. Social / financial status;

II. MONITORING

The Company gathers information about the Customer risk profile and expected behaviour when the Customer applies for Company's services. The gathered information provides information about the expected behaviour of the Customer and a baseline for identification of suspicious activity.

When suspicious activity is identified, or the Customer otherwise has a suspicious behaviour or pattern that indicates a risk for money laundering, the Company shall seek to investigate the behaviour and to provide a rationale for the identified

suspicious behaviour by asking the Customer for additional information to rule out inappropriate behaviour or attempt to launder money.

III. GEOGRAPHY RISK

CBRO UAB screen all customers and entities, CEO and UBO against PEP and Sanctions lists.

Negative risk impact factors:

a. If a country is subject of EU sanctions.
b. The country is one of the countries on the list of high risk and other monitored jurisdictions published by and the Financial Action Task Force (http://www.fatf-gafi.org/countries/)
c. The country on the list of third countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing frameworks published by the European Commission
d. Has a weak or non-existent AML/CTF legislation.
e. Has a high Corruption Perception Index.

IV. REPORTING

The Responsible Employee of the Company shall submit a written report at least once a year to the CEO of the Company about the execution of functions related to prevention of money laundering and / or terrorist financing. The Company shall, upon assessment of the threat posed by money laundering and/or terrorist financing, decide on the appropriateness of forwarding a report on a suspicious monetary operation or transaction to the Financial Crime Investigation Service of the Republic of Lithuania.

V. RECORDS

Records of the results of the investigation of complex or unusually large transactions and unusual patterns of transactions shall be stored for 5 years in paper or electronic form. The storage period may be extended for a maximum period of 2 years, when there is a motivated reason provided by the competent authority. The documents and information referred to shall be stored, regardless of whether the monetary transactions or transactions are domestic or international; business relations with the Customer are ongoing or have expired. Moreover, the documents and information referred to shall be stored in such a way as to enable the recovery of specific monetary transactions or transactions, and to provide the information contained therein, if necessary, to the FCIS or other competent authorities.

VI. DATA PROTECTION

a. The exchange of information is permitted only to prevent money laundering and terrorist financing.
b. Exceptions to the transmission of the information provided are not valid if a separate decision of the European Commission has been adopted.
c. When exchanging information with entities registered in third countries and providing personal data to these entities, the provision of personal data must comply with the requirements of the laws protecting personal data.
d. The Company or its employees are not liable for the breach of contractual obligations or damage to the Customer if this is due to a monetary operation or a suspension of a transaction.
e. Employees of the Company who are willing to notify the FCIS of suspicious monetary transactions or transactions executed by the Customer shall not be held liable.

VII. SUMMARY

These Rules may be amended, supplemented, or revoked by decision of the CEO of the Company.

These Rules shall be reviewed periodically (at least once a year) or upon any substantial events related to the operation of the Company or changes to applicable laws and shall be amended accordingly to ensure proper implementation of the money laundering and terrorist financing prevention measures, its effectiveness and relevancy. The Responsible Employee is responsible for the timely revision of the Rules and the preparation and submission of draft amendments to the CEO.

The Company conducts special training for the employees of the Company on issues related to the prevention of money and terrorist financing, as well as the proper implementation of these Rules