ANTI-MONEY LAUNDERING POLICY

1. APPLICATION

1.1. The Company provides services to individual and corporate customers and may receive online payments for its services. The Company engages the contractors and pays for their services, including by means of online payments. This Policy lays out principles and procedures to identify Company's customers and contractors in order to actively prevent money laundering and financing of terrorist or criminal activities.

1.2. This Policy applies to the Company's customers and contractors.

2. CUSTOMER AND CONTRACTOR DUE DILIGENCE

2.1. The Company shall apply customer and contractor due diligence procedures:

2.1.1. When establishing a business relationship with a contractor;
2.1.2. When carrying out an occasional transaction which
2.1.2.1. amounts to an amount equal to or higher than fifteen thousand euros (€15,000) whether the transaction is carried out in a single operation or in several operations which appear to be linked; or
2.1.2.2. exceeds one thousand euros (€1.000) and is at least partially carried out by electronic means through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics;
2.1.3. When there is a suspicion of money laundering or terrorist financing, regardless of the amount;
2.1.4. When there are doubts about the veracity or adequacy of previously obtained customer or contractor identification data.

2.2. The Company may appoint a compliance officer or engage KYC/AML service provider for the purposes of customer and contractor due diligence. Hereinafter "compliance officer" means either a compliance officer or KYC/AML service provider.

2.3. Standard customer and contractor due diligence process:

2.3.1. The customer or contractor is asked to provide identifying information:
2.3.1.1. For an individual: full name, citizenship, a copy of identification document (passport, etc.) and photo, post address;
2.3.1.2. For a legal entity: full name, jurisdiction of incorporation and registration No., post address.
2.3.2. The compliance officer verifies the information and documents provided; the compliance officer may use automated means for such verification. The compliance officer may use other data, such as the customer's or contractor's IP address and other metadata, to verify the identity of the customer or contractor.
2.3.3. The compliance officer performs search regarding the customer or contractor in question against the UN, EU or Cypriot sanctions lists, terrorist lists, politically exposed persons lists (collectively the "Watchlists Databases") to ensure that the customer or contractor in question is not subject to any sanctions administered or enforced by the United Nations Security Council, the European Union, or any other governmental authority with jurisdiction over the Company, and does not qualify as politically exposed person.

2.4. Enhanced due diligence is carried out if the compliance officer identifies one of the following risks:

2.4.1. legal person is incorporated or has a postal address in a jurisdiction included in the EU list of non-cooperative jurisdictions for tax purposes;
2.4.2. customer or contractor uses for paying to the Company or to receive a payment from the Company an account in a bank or payment institution included in the EU list of non-cooperative jurisdictions for tax purposes;
2.4.3. customer or contractor is incorporated in, is a citizen of or has a post address in a jurisdiction included in FATF list of high- risk and other monitored jurisdictions or a country designated by the Commission as presenting strategical shortcomings in its national system for combating money laundering and terrorist financing which are considered as important threats for the financial system of the European Union (hereinafter a "High Risk Country");
2.4.4. When there is a suspicion of money laundering or terrorist financing, regardless of the amount;
2.4.5. When there are doubts about the veracity or adequacy of previously obtained customer or contractor identification data.

2.5. If the compliance officer identifies one of the risks listed in clause 2.4 with respect to a customer or contractor, the compliance officer shall conduct enhanced due diligence for such customer or contractor. The scope of enhanced due diligence is determined on a case by case basis by the compliance officer and may involve request of documentary proof of information provided, information regarding beneficial owners of a legal entity, personal real-life identification by the Company or an institution subject to EU KYC/AML legislation and other measures.

2.6. If the customer or contractor due diligence is not successful, the compliance officer informs the legal and financial department of the Company, and the Company shall cease relationship with such customer or contractor. In case of the customer the Company notifies the customer of the contract termination and

refunds all amounts prepaid to the customer.

2.7. In event the compliance officer finds suspicious information or documents provided by a customer or contractor that indicated possible money laundering, terrorist financing activity or any other suspicious activity, the Company shall report the activity in accordance with applicable laws and regulations to the respective authority (if necessary).

3. RECORD KEEPING

3.1. The Company shall keep records of all due diligence checks, including:

3.1.1. information and documents requested and received in the course of due diligence;
3.1.2. messages, logs and metadata regarding the customer's or contractor's identification by automated means;
3.1.3. the status of the customer or contractor assigned as a result of due diligence procedures.

4. USEFUL RESOURCES

The following resources may be used to facilitate the due diligence procedures. Only authentic texts of legal acts published in official publication sources may be used as a basis for any decisions with legal implications.

4.1. United Nations Security Sanctions List Search: https://scsanctions.un.org/search/

4.2. EU Sanctions Map: www.sanctionsmap.eu

4.3. Lists of targeted persons and entities subject to EU Restrictive Measures (financial sanctions): http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm

4.4. The Official Journal of the EU. As of 01 July 2013, pursuant to Regulation (EU) No. 216/2013, the electronic version of the Official Journal of the EU is considered to be authentic and thus it has legal effect: http://eur-lex.europa.eu/JOIndex.do?ihmlang=en

4.5. The website of the EU where the countries subject to EU restrictive measures are listed: http://eeas.europa.eu/cfsp/sanctions/index_en.htm