# ANTI-MONEY LAUNDERING AND ANTI-TERRORISM POLICY

*PREMISE*

Mediasoft Studios S.r.l.s. (Mediasoft) through Bitcoin PosPAY, as a provider of services relating to the use of virtual currency and in compliance with the regulatory provisions on anti-money laundering and international terrorist financing (see Legislative Decree no. 231/2007 - "Anti-Money Laundering Decree"), has implemented suitable safeguards for the management of the related risk aimed at preventing the involvement of Mediasoft itself in criminal events that may have negative repercussions on its stability and reputation on the market.

Money laundering and terrorist financing represent criminal phenomena which, also by virtue of their transnational dimension, can pose a serious threat to the legal economy. These are highly polluting factors for the entire economic system: the reinvestment of illicit proceeds in legal activities and the presence of operators and economic organizations colluding with crime profoundly alter the market mechanisms, undermine the efficiency and correctness of the financial activity and weaken the economic system.

It is known that Mediasoft provides the activities of service provider relating to the use of virtual currency, through the provision to its users, registered on the website, of functional services for the acceptance of payments made in virtual currency and relating to goods and/or services. In this context, transactions that are protected through cryptography, potentially vulnerable, due to their pseudo anonymity, to the infiltration of money laundering and international terrorist financing phenomena, as indicated by the International Financial Action Group (FATF), or FATF (Financial Action Task Force).

Having said all this, Mediasoft's action to prevent and combat money laundering and terrorist financing is carried out through the introduction of third-party safeguards aimed at guaranteeing customer due diligence, traceability of financial transactions, identification of suspicious transactions and storage of customer data and documents. This document ("AML Policy"), in particular, describes the general principles and criteria - in turn subject to further and punctual internal regulation - implemented and managed by Mediasoft for the fulfillment of the obligations imposed by the Anti-Money Laundering Decree by reason of its characteristic activity, to which employees, collaborators, customers, company representatives and commercial partners are required to comply.

## *REGULATORY SOURCES*

Following the transposition into our legal system of Directive 2015/849/EU (known as the IV anti-money laundering directive), the national legislation on the subject has been substantially modified, extending its scope of application also to service providers relating to the use of virtual currency, limited to the performance of the conversion of virtual currencies from or into fiat currencies.

The IV Anti-Money Laundering Directive was implemented in our legal system with the Legislative Decree 90/2017 which amended and integrated the Anti-Money Laundering Decree.

The Anti-Money Laundering Decree is based on three main pillars:

- customer due diligence;
- storage of customer data and information;
- suspicious transaction reports.

The regulatory provisions of the Anti-Money Laundering Decree provide for an accurate census of customer information and introduce the concept of "risk-based approach" according to the "sensitivity" of customers, commensurate the customer due diligence obligations to the risk associated with the customer, the product and the geographical area.

The national authorities called to supervise compliance with the legislation are the Ministry of the Economy of Finance, the Financial Information Office (UIF) at the Bank of Italy, the Supervisory Authorities of the individual sectors in which the subject subjects operate. to the application of the legislation, the Anti-Mafia Investigation Department (DIA) and the Guardia di Finanza.

## *DEFINITIONS*

In order to clarify the terminology used in this AML/KYC Policy, the following definitions are specified:

- Client : It is the person who establishes ongoing relationships with Mediasoft, opens an account on the Site and carries out conversion operations or requests or obtains the execution of a professional service by Mediasoft.
- Identification Data : They are: the name and surname, the place and date of birth, the registered residence and the domicile, where different from the registered residence, the details of the identification document and, where assigned, the tax code or, in the case of subjects other than a natural person, the name, the registered office and, where assigned, the tax code.
- Executor : It is the person delegated to operate in the name and on behalf of the Customer or to whom powers of representation are conferred that allow him to operate in the name and on behalf of the Customer.

- Financing of Terrorism : Any activity directed, by any means, to the supply, collection, provision, intermediation, deposit, custody or disbursement, in any way realized, of funds and economic resources, directly or indirectly, in whole or in part, usable for carrying out one or more conducts, with the purpose of terrorism in accordance with the provisions of criminal laws, regardless of the actual use of funds and economic resources for the commission of the aforementioned conducts.
- Fractional Operation : It is a unitary operation in terms of economic value, for an amount equal to or greater than the limits established by this decree, carried out through several operations, individually lower than the aforementioned limits, carried out at different times and in a limited period of time fixed in seven days, without prejudice to the existence of the split operation when there are elements to consider it as such.
- Occasional Transaction : This is an operation that cannot be traced back to an ongoing relationship in place; the intellectual or commercial service, including those with instant execution, rendered in favor of the customer is also an occasional operation.
- High Risk Countries : These are the countries not belonging to the European Union whose legal systems have strategic deficiencies in their respective national systems for the prevention of money laundering and terrorist financing, as identified by the European Commission.
- Politically Exposed Persons - PEP : These are natural persons who have occupied or have ceased to occupy important public offices for less than a year, as well as their family members and those who are known to have close ties with the aforementioned subjects, as listed below:

1. are natural persons who hold or have occupied important public offices those who hold or have held the office of:

1. President of the Republic, President of the Council, Minister, Vice-Minister and Undersecretary, President of the Region, Regional Councilor, Mayor of a provincial capital or metropolitan city, Mayor of a municipality with a population of no less than 15,000 inhabitants and similar positions in foreign countries;
2. deputy, senator, European parliamentarian, regional councilor as well as similar positions in foreign states;
3. member of the central governing bodies of political parties;
4. judge of the Constitutional Court, magistrate of the Court of Cassation or of the Court of Auditors, councilor of state and other members of the Administrative Justice Council for the Sicilian Region as well as similar positions in foreign countries;
5. member of the governing bodies of central banks and independent authorities;
6. ambassador, person in charge of affairs or equivalent positions in foreign states, senior officer of the armed forces or similar positions in foreign states;
7. member of the administrative, management or control bodies of companies controlled, even indirectly, by the Italian State or by a foreign State or in which the Regions, provincial capitals and metropolitan cities and municipalities with a total population are held not less than 15,000 inhabitants;
8. general manager of ASL and hospital company, university hospital company and other bodies of the national health service;
9. director, deputy director and member of the management body or person performing equivalent functions in international organizations;

2. are family members of politically exposed persons: the parents, the spouse or the person linked in a civil union or de facto cohabitation or institutions similar to the politically

exposed person, the children and their spouses as well as the persons linked to the children in a civil union or de facto cohabitation or similar institutions;

3. are subjects with whom politically exposed persons are known to have close ties:

1. natural persons linked to the politically exposed person due to the joint beneficial ownership of legal entities or other close business relationships;
2. natural persons who only formally hold total control of an entity known to be established, in fact, in the interest and for the benefit of a politically exposed person.

- Continuous Relationship : It is a relationship of duration, falling within the exercise of the institute activity carried out by the obliged subjects, which does not end in a single operation.
- Laundering : Laundering means the following criminal phenomena: conversion or transfer of assets, carried out with the knowledge that they come from a criminal activity or from a participation in such activity, in order to conceal or conceal the illicit origin of the assets themselves o to help anyone involved in this activity to escape the legal consequences of their actions; concealment or concealment of the real nature, provenance, location, disposition, movement, ownership of the goods or of the rights thereon, carried out knowing that such goods come from a criminal activity or from a participation in such activity; purchase, possession or use of assets being aware, at the time of their receipt, that such assets come from a criminal activity or from a participation in such activity; d) participation in one of the acts referred to in letters a), b) and c) the association to commit this act, the attempt to perpetrate it, the fact of helping, instigating or advising someone to commit it or the fact of facilitating it execution.
- Effective Owner : It is the natural person or natural persons, other than the customer, in the interest of or of whom, in the last resort, the ongoing relationship is established, the professional service is rendered or the operation is performed.

## *DUE CUSTOMER VERIFICATION*

Customer knowledge ( know your customer - KYC) represents an essential issue of national and European legislation in the context of financial relations between operators and customers.

Adequate customer verification, in addition to constituting a valid tool for combating money laundering and terrorist financing, protects operators from exposure to commercial and reputational risks as well as from the application of administrative, civil and criminal sanctions.

Mediasoft carries out customer due diligence and monitors activity by analyzing the following parameters:

- identification data/generality;
- legal nature (for entities);
- prevalent activity carried out;
- origin of the funds;
- conduct at the time of the opening of the ongoing relationship or at the completion of the transaction;
- geographical area of belonging;

- purpose of opening the relationship;
- type of transaction or relationship;
- amount of the transaction;
- reasonableness of the transaction and of the relationship.

In acquiring information on customers, Mediasoft makes use of the activities carried out by third parties to whom the due diligence activity has been delegated. In particular, the delegated subject acquires at least the client's identification document and verifies its identity. In any case, the acquisition of internal and external data allows Mediasoft to be able to determine the related money laundering risk profile for each customer, which will be subjected to periodic monitoring based on the aforementioned risk profile.

During the relationship with the customer Mediasoft constantly updates the due diligence customer both during the review phase of the relationship (scheduled according to the level of risk), and upon the occurrence of any events such as by way of example and not limited to: the generation of anomalies detected by the IT applications in use, the reporting by the Authorities, the recognition of transactions entered into by the customer that are inconsistent with the nature of the underlying relationship.

### *COMPLIANCE WITH THE MAIN OBLIGATIONS REGARDING ANTI-MONEY LAUNDERING AND TERRORISM FINANCING*

The Anti-Money Laundering Policy adopted by Mediasoft is inspired by the principles of the "risk-based approach". In particular, Mediasoft:

- does not carry out transactions with shell banks that do not have a physical presence in the country in which they are established and authorized to carry out the activity ( shell bank );
- pays greater attention and adopts reinforced measures in cases in which situations arise that involve a greater risk of money laundering or in the verification of persons who hold or have held important public offices (Politically exposed persons);
- does not carry out operations that involve for any reason (presenters, orderers or beneficiaries) subjects registered in provisions of the judicial authorities;
- checks outbound and inbound operations (checks on beneficiaries and payers) and evaluates movements discarded following indices of similarity with anti-terrorism lists;
- carries out, in an automated way, personal data checks and makes comparisons with the names present in the lists provided by the UN and by the EC Regulations and by other international and national agencies.

### *RETENTION OF INFORMATION*

In order to comply with the conservation obligations, Mediasoft has set up an IT register, which ensures that the data is managed with clarity, completeness, so that

there is the immediacy of the information and the ease in consulting it. The keeping of the register was entrusted by Mediasoft to a third party.

The information and data found are kept for ten years as required by the current legislative decree 231/2007.

### *ANTI-MONEY LAUNDERING FUNCTION*

Mediasoft uses an external partner as Head of the Anti-Money Laundering Function.

In any case, Mediasoft's internal control system involves the entire corporate structure from the corporate bodies to the control functions. Mediasoft ensures that adequate internal controls are maintained to protect the integrity of the money laundering risk management process and the related reputational risk through the preparation of stringent guidelines on the subject, as well as through an adequate internal organizational structure.

The updating of the Anti-Money Laundering Policy, as well as the verification of compliance with the internal procedures and provisions adopted by Mediasoft, is entrusted to the Anti-Money Laundering Function which, in collaboration with the other internal functions or external professions, is called upon to guarantee the effectiveness of the activities. implemented to mitigate the risks associated with money laundering and the financing of terrorism.

### *ORGANIZATIONAL/REGULATORY PRESIDIA*

Mediasoft has implemented specific organizational/regulatory safeguards for the fulfillment of the obligations imposed by the Anti-Money Laundering Decree. In particular, adequate internal regulatory procedures have been prepared to regulate the obligations prescribed in order to provide the company functions of Mediasoft with organic consultation and support tools useful for understanding the matter.

Furthermore, Mediasoft has equipped itself with specific IT tools both for the analysis of the anti-money laundering risk profiles to be attributed to customers and for the monitoring of "anomalous" transactions for which an analysis is carried out by the competent structures in order to evaluation of the same.

### *REPORTING OF SUSPECTED TRANSACTIONS*

Mediasoft in order to cooperate with the Authorities to guarantee the stability of the financial system and avoid its involvement in money laundering and terrorist financing, has adopted a structured process for the reporting of transactions that arouse suspicion about the illicit origin of the transferred funds . For this purpose, Mediasoft has identified a person delegated to report suspicious transactions, who is required to transmit the reports to the Financial Intelligence Unit (UIF) in the forms and in the manner prescribed by the Authority.

*TRAINING*

Mediasoft, as required by the Anti-Money Laundering Decree, annually prepares a training program (e-learning, specialized courses) which is mandatory for all staff, collaborators and company representatives.