GreenVolt

Anti Money Laundering and Counter Terrorism Financing Policy

Shaped
by Nature

March 15, 2022

Anti Money Laundering and Counter Terrorism Financing Policy

The culture of GreenVolt - Energias Renováveis, SA ("**GreenVolt**") is based on values of transparency, accountability, and integrity, being absolutely committed to the active prevention and fight against money laundering and counter terrorist financing ("**ML&TF**").

This Anti Money Laundering and Counter Financing of Terrorism Policy (the "Policy") contains the guidelines to be adopted by GreenVolt and the companies integrated in its group ("**GreenVolt Group**") regarding the knowledge of the identity of the counterparty of its customers, suppliers, and partners who, in any way, have a relationship with them (hereinafter, individually, "**Customers**", "**Suppliers**" and "**Partners**"), with employees and members of governing bodies being essential elements to promote the values of the GreenVolt Group in the context of ML&TF.

1. Scope of application

The Policy is applicable to the entire GreenVolt Group, subject to the following rules:

(a) in the case of companies fully owned by GreenVolt, the respective management bodies must carry out the local transposition of this Policy;

(b) in the case of companies in which GreenVolt exercises control, co-control (Joint Ventures) or Significant Influence (Associates), the representatives of GreenVolt present in the management body must, as a result of the exercise of control, co-control, or Significant Influence, promote the adoption of the necessary measures for the local transposition of this Policy;

(c) in the case of companies in which GreenVolt does not exercise control or Significant Influence, GreenVolt representatives must observe the provisions of this Policy while carrying out their duties and, as far as possible, encourage the adoption of rules and procedures consistent with this Policy.

2. Legal Framework

This Policy is guided by the following regulations:

(a) Law No. 11/2002, of 16 February, which defines the criminal regime for non-compliance with financial or commercial sanctions imposed by a resolution of the United Nations Security Council or regulation of the European Union, which determine restrictions on the establishment or maintenance on the establishment or maintenance of financial or commercial relations with States, other entities or individuals, expressly identified in the respective subjective scope of incidence; and,

(b) Law No. 97/2017, of 23 August, which regulates the application and execution of restrictive measures approved by the United Nations or the European Union and establishes the sanctions applicable to the violation of these measures.

The sanctions mentioned in the aforementioned laws are a temporary restriction on the exercise of a certain right, through the imposition of a prohibition or obligation implemented by international organizations or by countries (individuals), which are applicable to jurisdictions, persons or entities with the aim of combat terrorism and maintain or restore international peace and security.

Compliance with this Policy does not affect the subjection of all companies in which GreenVolt participates to the applicable local legislation in terms of preventing and combating ML&TF, namely when they are considered "obliged entities" for the purposes of this same legislation, and suited risk models must be adopted to each of its legal, commercial, and operational realities.

3. ML&TF Risk Management Model

The ML&TF risk management model adopted favors a preventive approach based on the implementation of Know Your Client ("**KYC**"), Know Your Provider ("**KYP**") and Know Your Business Partner ("**KYBP**") procedures before the commencement of the commercial relationship, complemented with subsequent monitoring of possible future risks in strict articulation with the Company's Integrated Risk Management Policy.

4. Management Procedures and Risk Mitigation Actions

Prior to the establishment of a commercial relationship, the identification data of potential Customers, Suppliers and/or Partners and, when applicable, of their shareholders, legal representatives, and beneficial owners, must be screened against the external lists of Sanctions to identify increased risk situations ML&TF, using a screening tool ("**AML Screening**").

As part of the implementation procedure of this Policy, interlocutors with Customers, Suppliers and/or Partners must collect the information elements considered necessary in terms of counterparty knowledge, which may include, in the case of legal persons, the ownership structure and/or other form of control of the potential Customer, Supplier and/or Partner.

The information collected prior to the start of the business relationship must be updated in the following situations:

(i) Whenever it is suspected that the Client, Supplier and/or Partner and, consequently, their commercial activities, may be related, directly or indirectly, to the practice of ML&TF crimes or the application of Sanctions;

(ii) Whenever there are doubts about the accuracy or adequacy of identification elements previously obtained from the Client, Supplier and/or Partner and, if applicable, from their beneficial owners and legal representatives;

(iii) Whenever GreenVolt becomes aware, through the Customer, Supplier and/or Partner, or their governing bodies, that there have been or will be significant changes: i) in the identity; ii) business strategy (industry or geography of operations); or iii) the shareholders and/or members of the structure owned by the Client and/or Third Party;

(iv) Whenever GreenVolt becomes aware that the Customer, Supplier and/or Partner, or their beneficial owners or legal representatives, have been subject to sanctions.

As a result of the information obtained under the terms of the previous paragraphs, GreenVolt shall consider the maintenance and/or establishment of business relationships with the Customers, Suppliers and/or Partners in question.

5. Complaints on AML&TF maters

GreenVolt's Internal Whistleblower Policy regulates the specific and independent channels that, internally, ensure the reception, treatment and filing of communications of irregularities related to this Policy.

6. Disclosure

This Policy is disclosed to employees and members of the governing bodies of the GreenVolt Group.

7. Final dispositions

This Policy enters into force on the date of its approval by the Board of Directors.

Any change to this Policy must be approved by the Board of Directors, with the powers of delegation to the managing director, with regard to the necessary changes to conform the Policy with the legislation in force at any given time.

APPENDIX I

DEFINITIONS

1. "**Associate**" means an entity, with or without legal personality, over which a person exercises significant influence, provided that it is not a Subsidiary.
2. "**Money laundering**" consists of the conversion, transfer, assistance or facilitation of any transaction of conversion or transfer of advantages - obtained by itself or by a third party, directly or indirectly - arising from the practice of a certain set of criminal offenses, with the aim of to conceal the unlawful origin of these benefits, or to prevent the perpetrator or participant of these offenses from being criminally prosecuted or subjected to a criminal reaction, or camouflage or concealment of the true nature, origin, location, disposition, movement or ownership of the advantages arising from the practice of preceding crimes, or corresponding rights.
3. "**Terrorist Financing**" consists of the supply, collection or holding (directly or indirectly) of funds or goods of any kind, as well as products or rights that can be transformed into funds, intended to be used or knowing that they can be used (fully or partially):

   1. In planning, preparing, or practicing the following facts:

   (a) a) Crimes against the life, physical integrity, or liberty of persons;

   (b) b) Crimes against the security of transport and communications, including information technology, telegraph, telephone, radio, or television;

   (c) c) Crimes of intentional production of common danger, through fire, explosion, release of radioactive substances or toxic or asphyxiating gases, flood or avalanche, collapse of construction, contamination of food and water intended for human consumption or spread of disease, harmful pest, plant, or animal;

   (d) Acts that destroy or make it impossible to function or deviate from their normal purposes, definitively or temporarily, totally, or partially, means or means of communication, public service facilities or intended to supply and satisfy the vital needs of the population;

(e) Research and development of biological or chemical weapons;

(f) Crimes involving the use of nuclear energy, firearms, biological or chemical weapons, explosive substances or devices, incendiary means of any nature, parcels, or booby-trapped letters; whenever, by their nature or the context in which they are practiced, these facts are likely to seriously affect the state or the population that is intended to be intimidated, with the intention of

- harm national integrity and independence, impede, alter or subvert the functioning of State institutions provided for in the Constitution, force public authority to perform an act, refrain from performing it or tolerate it being performed, or intimidate certain persons, groups of persons or the general population, or impair the integrity or independence of a State, impede, alter or subvert the functioning of the institutions of that State or of a public international organization, force the respective authorities to perform an act, to refrain from practicing it or to tolerate its practice, or even to intimidate certain groups of people or populations.

2. In planning, preparing, or practicing the following facts:

(a) Dissemination, to the public, of a message encouraging the practice of the facts referred to in paragraph 1;

(b) Recruitment of third parties to carry out the acts referred to in paragraph 1;

(c) Provision, receipt or acquisition of training, instruction or knowledge on the manufacture or use of explosives/firearms or other weapons/harmful or dangerous substances/other specific methods and techniques, for the practice of the facts referred to in no. 1;

(d) Carrying out or attempting to travel to a territory other than the State of residence or nationality, with the aim of providing, receiving, or acquiring logistical support, training, instruction or knowledge on the manufacture or use of explosives/firearms or other weapons/ harmful or dangerous substances/other specific methods and techniques, for the practice of the acts referred to in paragraph 1;

(e) Carrying out or attempting to travel to a territory other than the State of residence or nationality, with the aim of joining a terrorist organization or committing the acts referred to in paragraph 1;

(f) Organization or facilitation of travel or attempted travel provided for in the preceding paragraphs d) and e).

4. "**Significant Influence**" means the power to participate in the decisions of the financial and operating policies of the investee or of an economic activity, but which is neither Control nor Joint Control over those policies. Significant Influence can be obtained through ownership of stock, by-laws, or agreement.