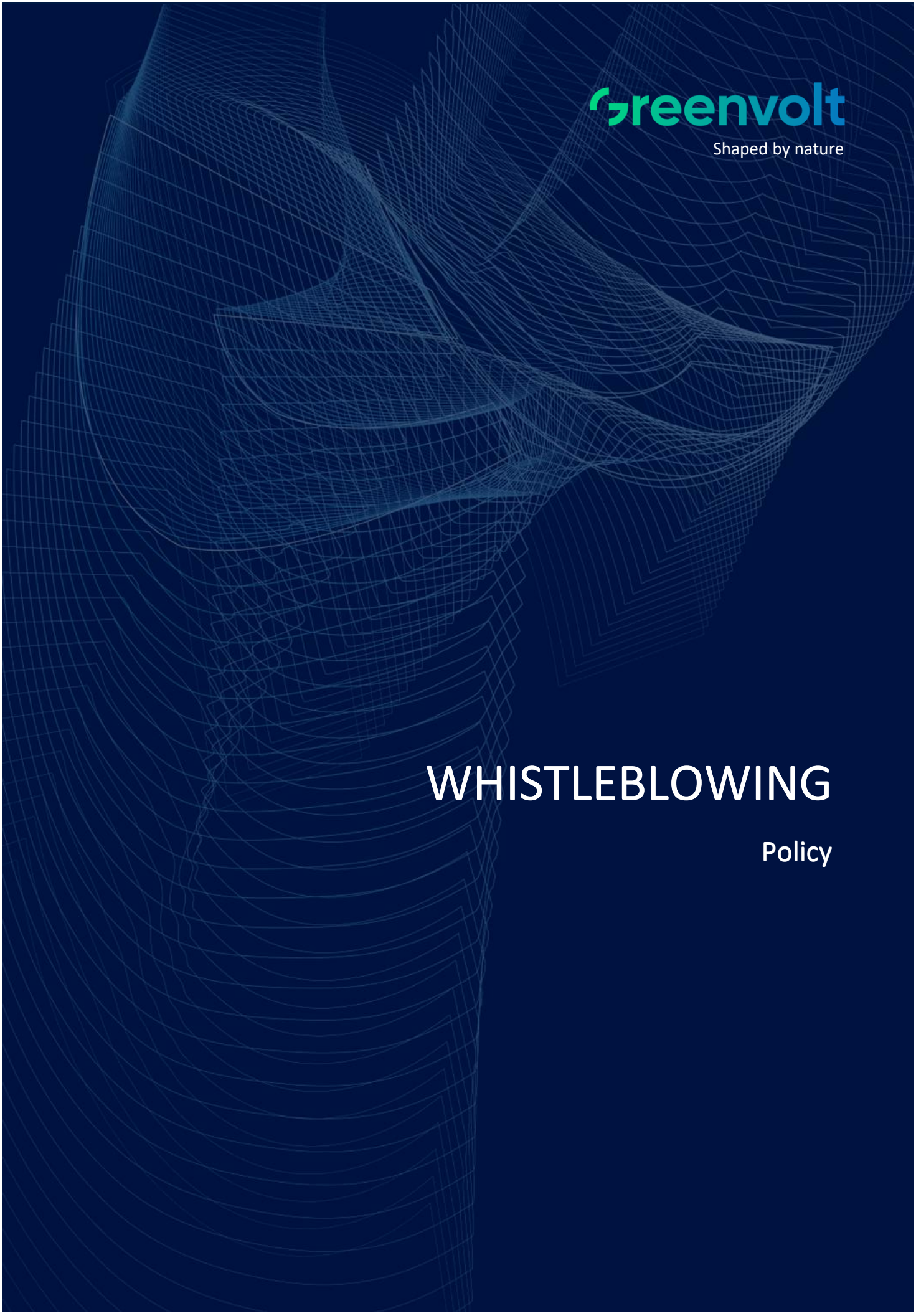

WHISTLEBLOWING

Policy

Page intentionally left blank

Index

Version History

Version	Date of Approval	Elaboration	Approval	Remarks
1	15 March 2022	Legal Directorate	Greenvolt Group Board of Directors	Initial emission
2	21 July 2023	Assurance Compliance and Efficiency	Greenvolt Group CEO	Changes to channels for receiving requests and internal mechanisms for handling complaints

1. Introduction

Greenvolt - Energias Renováveis S.A. and its subsidiaries (hereinafter jointly referred to as the "Greenvolt Group") strive for an organisational culture of transparency, based on the highest ethical standards of conduct, through the establishment of channels that, guaranteeing anonymity and confidentiality of communication, allow all employees, members of corporate bodies and service providers to Report[1] Breaches and Irregularities of which they are aware.

2. Objective

The purpose of this policy (the "Policy") is to define the internal rules and procedures for receiving, processing, and dealing with the Reporting of Breaches and Irregularities within the Greenvolt Group.

3. Scope

For the purposes of this Policy the following definitions are considered:

a) Breach means any act or omission contrary to the rules contained in the European Union acts referred to in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council, national rules implementing, transposing or enforcing such acts or any other rules contained in legislative acts implementing or transposing the aforementioned Directive, including those providing for criminal offences or administrative offences, relating to the areas identified in Annex I to this Policy ("Breach"); and

b) Irregularity means all acts or omissions which, even if they do not fall within the definition of a Breach, are contrary to national, European, international, or internal laws, regulations, and recommendations of the Greenvolt Group, including, without limitation, in the field of accounting, auditing, internal control and the fight against corruption and financial crimes of any kind ("Irregularity").

The Policy is applicable to all natural persons who have access to information, in the course of their professional activity, regardless of the nature of this activity and the sector in which it is carried out, in relation to the Greenvolt Group.

[1] Oral or written communication of information on Breaches and Irregularities.

The Policy is applicable, without prejudice to the particular legal framework of the respective geographies, to the entire Greenvolt Group.

In the case of companies in which Greenvolt exercises control, co-control (Joint Ventures or Joint-Venture) or Significant Influence[2] , the representatives of Greenvolt present in the management body must, by effect of the exercise of control, co-control, or Significant Influence, promote the adoption of the necessary measures for the local transposition of this Policy.

In the case of companies in which Greenvolt does not exercise control or Significant Influence, Greenvolt's representatives shall comply with the provisions of this Policy in the performance of their duties and, to the extent possible, encourage the adoption of rules and procedures consistent with this Policy.

4. Principles

The Policy is governed by the following Principles:

4.1. Confidentiality of the Identity of the Reporting Person and the Person Concerned

The identity of the Reporting Person[3] and of the Person Concerned[4] , as well as the information that may allow their identification, are confidential in nature, and are restricted to the persons responsible for receiving and/or following up on the Reports. The obligation of confidentiality applies to all persons who have received information about the Reports.

The identity of the Reporting Person and the Person Concerned may only be disclosed as a result of a legal obligation or judicial decision, preceded by written communication to the Reporting Person

[2] The power to participate in decisions about the financial and operating policies of the investee or an economic activity, but which is not control or joint control over those policies. Significant Influence can be obtained by share ownership, status, or agreement.

[3] Any natural person who reports a Breach or Irregularity based on information obtained in the course of their professional activity (even if it has ceased in the meantime, in the recruitment phase or in the pre-contractual negotiation phase) carried out within the Greenvolt Group or in their interaction with the entities that constitute the same, regardless of the nature of this activity and the area or department in which it is carried out, namely employees, service providers, contractors, subcontractors and suppliers and any persons acting under their direction or supervision, holders of shareholdings, persons belonging to Greenvolt's administrative, management, fiscal or supervisory bodies, volunteers and interns (paid or unpaid).

[4] The person named in the Report as the perpetrator of the Breach or to whom it is linked.

and/or the Person Concerned indicating the reasons for the disclosure, unless the provision of this information jeopardises the related investigations or judicial proceedings.

4.2. Conservation of Information

Reports submitted under the Policy are subject to registration and retention for a period of 5 years and, regardless of this period, during the pendency of judicial or administrative proceedings relating to the complaint, without prejudice to special rules on the protection of personal data, in particular data retention, provided for in internal policy.

4.3. Precedence of Internal Reporting

Whenever there is an Internal Reporting Channel available, as a rule, the Reporting Person cannot resort to external reporting channels beforehand.

4.4. Prohibition of Disclosure

As a rule, the Reporting Person may not publicly disclose a Breach or Irregularity or make it known to the media or journalist, and does not benefit from the protection afforded by the Policy, except in the cases provided for by law.

4.5. Prohibition of Retaliation for Reporting Breaches

In cases of Reports on Breaches, the Reporting Person, the Reporting Person's Assistant[5] and legal persons or similar entities owned or controlled by the Reporting Person, for which the Reporting Person works or with which the Reporting Person is otherwise connected in a professional context, may not be subject to Retaliatory Acts[6].

The following acts, when committed up to two years after a Report or public disclosure of a Breach, are presumed to be motivated by that same Report, until proven otherwise:

[5] The natural person who assists the Reporting Person in the Report procedure and whose assistance is to be confidential, including trade union representatives or employee representatives.

[6] An act or omission which, directly or indirectly, occurring in a professional context and motivated by the Reporting of a Breach under the Policy, unjustifiably causes or is likely to cause harm to the Reporting Person or threats or attempts to cause such acts and omissions.

i) Dismissal;
ii) Change in working conditions, such as duties, hours, place of work or pay, failure to promote the employee or failure to fulfil work duties;
iii) Suspension of the labour contract;
iv) Negative performance evaluation or negative reference for employment purposes;
v) Failure to convert a fixed-term employment contract into an open-ended contract where the employee had legitimate expectations of such conversion;
vi) Non-renewal of a fixed-term employment contract;
vii) Inclusion on a list, based on a sector-wide agreement, which may lead to the Reporting Person being unable to find employment in the sector or industry concerned in the future;
viii) Termination of a supply or service contract;

Any disciplinary sanction imposed on the Reporting Person and the Reporting Person's Assistant shall be presumed to be abusive until two years after the report has been lodged or made public.

4.6. Responsibility of the Reporting Person

The Reporting Person cannot be held disciplinary, civil, misdemeanour or criminally liable for reporting or publicly disclosing a Breach made under the Policy.

The Reporting Person cannot be held liable for obtaining or accessing the information that prompts the report or public disclosure, unless obtaining or accessing it constitutes a criminal offence.

4.7. Processing of Personal Data

The purpose of processing the information communicated under this Policy is to receive and follow up on Reports submitted to the Internal Reporting Channels, and personal data that are clearly not relevant to the processing of the Report will not be kept and will be immediately deleted.

The right of information is guaranteed, in accordance with the law, in particular regarding the entity responsible for receiving and processing the Report, the facts reported and the purpose of processing the information received, as well as the right to access and rectify the personal data.

Under data protection and information security rules, appropriate security measures must be in place to protect the information and data contained in the Reports and the corresponding registers.

5. Internal Reporting Channels

Internal Reports can be sent via this link, which is available on the various Greenvolt Group websites as well as on the Intranet.

The instructions for using the Internal Reporting Channels can be consulted at any time as they will also be available at the above-mentioned locations.

6. Procedure for managing Reports

The following procedure should be followed for handling Reports received through the channels mentioned in the previous section:

- The Corporate *Compliance* Area (hereinafter "*Compliance*") must ensure the receipt, investigation, and follow-up of Reports, ensuring the inclusion of the competent corporate structures, depending on the subject of the respective Breach or Irregularity, and following the procedures defined within the scope of internal investigations, ensuring compliance with the following processes and deadlines:

- Within seven (7) days of receipt of a Report through the Internal Reporting Channels, *Compliance* notifies the Reporting Person of its receipt with information on the requirements, competent authorities, form, and admissibility of the external complaint.

- Within a maximum period of two (2) months following the receipt of a Report through the Internal Reporting Channels, *Compliance,* with the support of the competent corporate structures, shall produce a written document containing the analysis of the Report, the description of the internal actions taken and the conclusions reached, including, if deemed necessary, the opening of an internal investigation or the communication to the competent authority for the investigation of the Breach or Irregularity.

- Within a maximum of three (3) months following the receipt of a Report through the Internal Communication Channels, *Compliance* informs the Reporting Person of the follow-up given to the Report and of the actions and measures implemented to address the facts and information reported therein.

- The Reporting Person may request to be informed of the outcome of the analysis carried out on the Report within fifteen (15) days of its conclusion.

- If an internal investigation is opened, once all the investigative procedures have been completed, a report should be drawn up detailing the case reported, the steps taken in the investigation, as well as the measures adopted to mitigate the risk identified and prevent the recurrence of the Breaches or Irregularities reported.

- *Compliance* and the corporate structures involved in the process may be assisted by internal or external entities designated by them, such persons being bound by the applicable duty of confidentiality.

7. Non-compliance

Failure to comply with the rules set out in this Policy is subject to the application of internal sanctions, adopting the applicable disciplinary and/or legal measures, without prejudice to the administrative and/or judicial liability that may be attributable, either to the individuals involved or to the company itself.

The possible misdemeanour liability of Greenvolt Group entities does not exclude the individual liability of natural persons.

8. Final Provisions

Compliance is responsible for monitoring the application of this Policy, as well as for reviewing it on a biennial basis or whenever there are relevant changes in the applicable legal framework and in the context of the activities carried out by Greenvolt and whenever new elements arise that demonstrate that it is not fully appropriate, submitting the proposed changes to the approval of the CEO of the Greenvolt Group.

Any amendment to this Policy must be approved by the Board of Directors of Greenvolt Group, with the power to delegate to the CEO of the Greenvolt Group, with regard to changes necessary to comply with the internal procedures established in this area.

This Policy shall enter into force on the date of its approval.

ANNEX I

For the purposes of the Policy, an Offence is considered to be:

(a) an act or omission contrary to rules contained in European Union acts referred to in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council, national rules implementing, transposing, or enforcing such acts or any other rules contained in legislative acts implementing or transposing them, including those providing for criminal offences or administrative offences, relating to the fields of:

i) Public procurement;

ii) Financial services, products and markets and prevention of money laundering and terrorist financing;

iii) Product safety and compliance;

(iv) Transport safety;

v) Protection of the environment;

vi) Radiation protection and nuclear safety;

vii) Food and feed safety, animal health and animal welfare;

viii) Public health;

ix) Consumer protection;

(x) Protection of privacy and personal data and security of network and information systems;

(b) an act or omission contrary to and detrimental to the financial interests of the European Union to which it relates Article 325 of the Treaty on the Functioning of the European Union (TFEU), as referred to in Article 3(1) of the Treaty on European Union (TFEU) specified in the applicable European Union measures;

(c) the act or omission contrary to the internal market rules referred to in Article 26(2) TFEU, including competition and state aid rules, as well as the rules of corporate taxation;

(d) an act or omission that contradicts the purpose of the rules or standards covered by points (a) to (c).