Protection of Personal Data Policy

Updated September 27, 2023

The Board of Directors of NEOENERGIA S.A. (the "**Society**") is vested with the powers to prepare, assess and review the Society's Governance and Sustainability System on an on-going basis and, specifically, to approve and update, the corporate policies, which contain the guidelines governing the conduct of the Society and the societies integrated into the group, whose dominant entity is, in the sense established by law, the Company ("Group")..

In the exercise of these powers, and within the legal framework, the Bylaws, the guidelines and rules of action in which the *Purpose and Values of the Neoenergia Group* are materialized, as well as its sustainable development strategy, the Board of Directors approves this *Personal Data Protection Policy* (the "*Policy*").

1. Purpose

The purpose of this *Policy* is to establish the general principles and common guidelines that shall govern operations within the Group's perimeter as regards personal data protection, ensuring compliance with applicable law under all circumstances.

Particularly, the *Policy* ensures the right to protection of personal data for all natural persons who establish relations with the societies of the Group, ensuring respect for the rights to reputation and to privacy in the processing of the various categories of personal data from different sources and for various purposes based on their business activities, all of which in compliance with the Group's *Human Rights Respect Policy.*

2. Scope

Within the limits established by law, this *Policy* is applicable to all societies comprising the Group and investees not comprising the Group, over which the Society has management influence.

For investees to which this *Policy* is not applicable, the Society shall promote, through its representatives on the management bodies of such societies, the alignment of their own policies with those of the Society.

This *Policy* shall also apply, as appropriate, to the joint ventures, temporary joint ventures and other equivalent associations, when the Society is responsible for the management thereof.

3. General principles for the processing of personal data

Group societies shall thoroughly comply with personal data protection law in their jurisdiction, the laws applicable to the processing of personal data carried out and the laws determined by binding rules or agreements adopted within the Group.

Group societies shall strive to ensure that the principles set forth in this *Policy* are considered (i) in the design and implementation of all procedures involving the processing of personal data, (ii) in the products and services offered thereby, (iii) in all agreements and obligations that they formalize with natural persons, and (iv) in the implementation of any systems and

platforms that allow access by employees of Group societies or third parties to personal data and/or the collection or processing of such data.

4. Basic principles for the processing of personal data

The principles related to the processing of personal data underpinning this *Policy* are described below:

a) *Principles of legitimate, lawful and fair* processing of personal data.

The processing of personal data shall be fair, legitimate and lawful in compliance with applicable law. In this sense, personal data shall be collected for one or more specific and legitimate purposes in compliance with applicable law.

When so required by law, the consent of the data subjects shall be obtained before their data is collected.

Also, when so required by law, the purposes for processing the personal data shall be explicit and specific at the time of collection thereof.

Particularly, Group societies shall not request or process personal data relating to ethnic or racial origin, political ideology, beliefs, religious or philosophical convictions, sexual orientation or practices, trade union membership, data concerning health, or genetic or biometric data for the purpose of uniquely identifying a person, unless the collection of said data is necessary, legitimate and required or permitted by applicable law, in which case they shall be collected and processed in compliance with the provisions thereof.

b) *Principle of minimization*

Only personal data that is strictly necessary for the purposes for which it is collected or processed and adequate for such purposes shall be processed.

c) *Principle* of accuracy.

Personal data must be accurate and up to date. Otherwise, such data shall be deleted or rectified.

d) *Principle* of limitation for the storage period.

Personal data shall not be stored for longer than is necessary for the purposes for which it is processed, except in the circumstances established by law.

e) *Principles* of integrity and confidentiality.

In processing personal data, adequate security shall be ensured through technical or organizational measures, to protect such data from unauthorized or unlawful processing and to prevent their loss, destruction, and accidental damage.

Personal data collected and processed by Group societies shall be stored with the utmost confidentiality and secrecy, may not be used for purposes other than those that justified and permitted the collection thereof, and may not be disclosed or transferred to third parties except in the cases permitted by applicable law.

f) *Principle* of proactive responsibility (accountability).

Group societies shall be responsible for complying with the principles set forth in this *Policy* and those required by applicable law and shall be able to evidence compliance when so required by applicable law.

Group societies shall perform a risk assessment of the processing carried out by them in order to identify the measures to be applied to ensure that personal data are processed in compliance with legal requirements. When so required by law, new products, services or IT systems shall be previously assessed for identifying the risks that may be posed to personal data protection and shall adopt the necessary measures to eliminate or mitigate them. Group societies shall maintain a record of activities in which they describe the personal data processing carried out by them in the course of their activities.

In the event of an incident causing the accidental or unlawful destruction, loss or change of personal data, or the disclosure of or unauthorized access to such data, the internal protocols established for such purpose by the Society's Corporate Security area (or by the area that, at any given moment, assumes its functions) and those established by applicable law must be followed. Such incidents shall be documented and measures shall be adopted to resolve and mitigate potential adverse effects for data subjects. In the cases provided for by law, Data Protection Officers (DPOs) shall be nominated, in order to ensure that Group societies comply with the legal provisions on data protection.

g) *Principles* of transparency and information.

The processing of personal data shall be transparent towards the data subject, providing intelligible and accessible information about the processing to data subjects regarding the processing of their data when so required by applicable law.

For purposes of ensuring fair and transparent processing, the Group society that is responsible for the processing shall inform data subjects whose data is to be collected of the circumstances relating to the processing in compliance with applicable law.

h) *Acquisition* or procurement of personal data.

It is forbidden to acquire or procure personal data from unlawful sources, from sources that do not evidence sufficient assurance the legitimate origin of such data or from sources whose data has been collected or transferred in violation of the law.

i) *Engagement* of data processors.

Prior to engaging any service provider that may have access to personal data for which Group societies are responsible, as well as during the effective term of the contractual relationship, such Group societies shall adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing by service provider is performed in compliance with applicable law.

j) *International transfers* of data.

Any processing of personal data that is subject to European Union regulations and entails a transfer of data outside the European Economic Area shall be carried out strictly in compliance with the requirements established by applicable law in the jurisdiction of origin. Group societies located outside the European Union shall comply with any requirements for international transfers of personal data applicable, as the case may be, in their respective jurisdictions.

k) *Rights* of data subjects.

Group societies shall allow data subjects to exercise the rights of access, rectification, deletion, restriction of processing, portability and objection that are applicable in each jurisdiction, establishing internal procedures for such purpose as may be necessary to at least meet the legal requirements applicable in each case.

5. Implementation

The Corporate Security area, together with the Society's Legal Services (or the areas that, at each moment, assume their functions),, shall develop and keep updated, pursuant to the provisions in this *Policy*, internal rules for global data protection management at the Group level, which shall be implemented by the Corporate Security Executive Office, and which shall be mandatory for all Society's officers and employees.

The Legal Services area or area in charge of such duties shall be responsible for informing the Society's Corporate Security area of regulatory developments and news occurred in this area.

The Society's Systems area, or area in charge of such duties, shall be responsible for implementing the information technology systems of the Group societies, as well as the information technology controls and developments that are appropriate to ensure compliance with the internal rules for global data protection management, and shall ensure that said developments are updated at all times.

In addition, the businesses and corporate divisions shall (i) subject to the provisions of applicable law in each case, appoint the persons responsible for the data, who shall act on a coordinated basis and under the supervision of the Society's Corporate Security area; and (ii) coordinate with the Corporate Security area (or the areas that, at each moment, assume their functions), any activity that involves or entails the management of personal data. Finally, the Cybersecurity Committee, (or the areas that, at each moment, assume their functions), created pursuant to the provisions of the Cybersecurity Risk Policy, shall monitor the general status of personal data protection at the Group societies and shall endeavor to ensure proper Group-level coordination of risk practices and management in the area of personal data protection, assisting the Corporate Security Executive Office in the approval of internal rules on cybersecurity and data protection.

6. Control and assessment

a) Control

The Corporate Security area, (or the areas that, at each moment, assume their functions),, shall supervise compliance with the provisions of this *Policy* by the Society and other Group societies. The foregoing shall in any event be without prejudice to the responsibilities vested in other bodies and areas of the Society and, if applicable, in the management bodies of the Group societies.

Regular audits shall be performed with internal or external auditors in order to assess compliance with this *Policy*.

b) Assessment

The Corporate Security area (or the areas that, at each moment, assume their functions),,shall assess compliance with and the effectiveness of this Policy at least once per year and shall report the results of such assessment to the Resources Executive Office, or to the area in charge of such duties at any time.

* * *

This Policy was initially approved by the Board of Directors on June 28, 2018 and last updated at the Board of Directors' Meeting held on September 27, 2023.