Personal Data Protection Policy

Updated on October 16th, 2025

NEOENERGIA S.A.'s (the "**Company**") Board of Directors has the power to prepare, evaluate and consistently review the Company's Governance and Sustainability System, as well as approve and update policies that contain guidelines that govern the Company's performance. They may also provide notice of, as applicable, the policies that, during the exercise of their autonomy, they decide to approve at companies that are part of the group where the dominant entity is, as established by law, the Company (the "**Group**").

In the exercise of these powers and within the scope of existing legislation, the Company's Articles of Incorporation and the Neoenergia Group's Corporate Purpose and Values, as well as its Sustainable Development Strategy, the Board of Directors hereby approves this Personal Data Protection Policy ("**the Policy**"). This Policy will respect, develop and adapt the Group's Core Ethical Principles of Governance and Sustainability.

1. Scope

This Policy is applicable to the Company. Nevertheless, this Policy describes the actions and regulatory developments that must be carried out by the other companies of the Group while observing their competencies and their autonomy.

These principles must also offer guidance, when applicable, for the performance of the Neoenergia Institute, which is linked to the Group.

The Company will promote the alignment of the regulations of the companies in which it holds an ownership interest, but which are not part of the Group, as well as joint ventures, temporary company associations and other entities it manages, with the principles contained in this Policy.

2. Purpose

The purpose of this Policy is to establish the principles that will govern the Company's performance in relation to the protection of personal data, to ensure consistent compliance with the applicable regulations.

In particular, this Policy guarantees the right to data protection among individuals who maintain relationships the Company. It ensures respect for the right to honor and privacy in the processing of different types of personal data from different sources and for different purposes depending on their business activities, all in compliance with the Human Rights Respect Policy.

3. Principles of action

The Company assumes and promotes the following principles of action, which must be part of its activities regarding the protection of personal data:

a) Principles of legitimacy, lawfulness and faithfulness during the processing of personal data: The processing of personal data must be fair, legitimate and lawful in accordance with applicable regulations. Personal data must therefore be collected for one or more specific and legitimate purposes in accordance with applicable regulations.

In cases in which data collection is mandatory according to applicable regulations, the Company must obtain the consent of the interested parties before requesting their data.

In a similar manner, whenever required by law, the purposes of the processing of personal data must be explicit and determined prior to collection.

In particular, the Company must not request or process personal data relating to ethnicity, political ideology, beliefs, religious or philosophical beliefs, sexual behavior or orientation, trade union membership, health, or genetic or biometric data aimed at uniquely identifying a person, unless the collection of such data is necessary, legitimate and required or permitted by applicable law. In such cases data will be requested and processed in accordance with the provisions of the corresponding law.

b) Minimization principle: Only personal data that are strictly necessary for the purpose for which they are collected or processed and suitable for such purposes will be processed.

c) *Accuracy principle* : Personal data must be accurate and up to date; otherwise, they must be deleted or rectified.

d) Principle of limited storage: Personal data must not be kept beyond the period necessary to achieve the purpose for which they are intended, except in the cases provided for by law.

e) Principles of integrity and confidentiality: When processing personal data, it will be necessary to ensure adequate security through technical or organizational measures that protects them from unauthorized or unlawful processing and prevents their loss, destruction and accidental damage.

Personal data requested and processed by the Company must be stored with the utmost confidentiality and secrecy and cannot be used for purposes other than those

for which they were justified and allowed to be collected. They must not be forwarded or assigned to third parties beyond the exceptions allowed under applicable regulations.

f) Principle of proactive responsibility (accountability): The Company shall be responsible for complying with the principles stipulated in this Policy and those required under applicable regulations. It must be able to demonstrate compliance when required by applicable law.

The Company must prepare a risk assessment of the processing it carries out in order to determine the measures to be applied to ensure that personal data are processed in accordance with legal requirements. In cases in which the law so requires, the risks that new products, services or information systems may entail for personal data protection will be assessed in advance, and the necessary measures will be taken to eliminate or mitigate them.

The Company must keep a record of the activities that describe the personal data that they process within the scope of their activities.

If an incident occurs that results in the accidental or unlawful destruction, loss or alteration of personal data, or the sending or unauthorized access to this data, the internal protocols established by the Corporate Security and Resilience department (or by the area that come to assumes its functions) must be observed through the Security, Resilience and Digital Technologies Committee and applicable legislation. These incidents must be documented and steps taken to address and minimize potential negative effects to stakeholders.

In the cases provided for by law, a Personal Data Protection Officer (DPO) will be appointed in order to ensure compliance with data protection standards at the Group's companies.

g) Principles of transparency and information: The processing of personal data will be transparent in relation to the interested party and information on the processing of their data will be provided in an understandable and accessible manner, when required by applicable laws.

In order to ensure fair and transparent processing, the Company must inform those affected or interested whose data is to be requested of the circumstances related to processing according to applicable regulations.

h) Acquisition or obtaining of personal data: It is prohibited that personal data be acquired or obtained from illegitimate sources, sources that do not sufficiently

guarantee their legitimate origin or those in which data have been requested or transferred in violation of the law.

i) Contracting of data processing operators: Prior to contracting any service provider that accesses personal data that is under the control of the Company, as well as during the term of the respective contractual relationship, the Company must adopt the necessary measures to ensure and, when legally required, demonstrate that data processing is performed by the operator in accordance with applicable legislation.

j) International data transfers: Any processing of personal data subject to European Union regulations that involves the transfer of data outside the European Economic Area must be carried out in strict compliance with the requirements established in the applicable law in the jurisdiction of origin.

k) Rights of interested parties: The Company must allow interested parties to exercise their rights of access, rectification, deletion, limitation of treatment, portability and opposition that are applicable at each location. It must establish, for this purpose, internal procedures that are necessary to satisfy, at a minimum, the legal requirements applicable in each case.

4. Coordination at Group level

The Security and Corporate Resilience department, through the Security, Resilience and Digital Technologies Committee (or the areas that come to assume their functions) will ensure the proper coordination, at Group level, of practices and risk management within the scope of the protection of personal data. It will establish the appropriate coordination procedures together with the security, resilience and digital technologies committees or with security department(or the committee or area that comes to assume its functions) at the Group.

The Legal Services department (or the area that comes to assume its functions) will be responsible for reporting the developments and regulatory news that occur in the scope of the protection of personal data. to the Security and Corporate Resilience area, through the Security, Resilience and Digital Technologies Committee (or the committee that comes to assume its functions)

Additionally, business and corporate boards must: (i) designate the persons responsible for personal data, who will act in coordination and under the supervision of the Security and Corporate Resilience department (or the area that comes to assume its functions) and the Security, Resilience and Digital Technologies Commission (or the committee that comes to assume its functions) and (ii) coordinate with the Security and Corporate Resilience department (or the area that comes to assume its functions) during any activity that implies or involves the processing of personal data.

5. Implementation and monitoring

As part of the implementation and monitoring of the provisions of this Policy, the Board of Directors relies on the Security and Corporate Resilience Department (or the area that comes to assume its functions) which, through the Security, Resilience and Digital Technologies Committee (or the committee that comes to assume its functions) will develop and keep up to date internal regulations for the management of personal data protection d, in accordance with the provisions of this Policy. The regulations will be implemented by the Security and Corporate Resilience area and will be mandatory for the members of the management team and all Group employees.

Without prejudice to the above provisions, it will be the responsibility of the Group's Digital Transformation department (or the area that comes to assume its functions) to ensure that the Group's information systems are correctly implemented. They must also ensure controls and computer developments are adequate to ensure compliance with internal data protection regulations and that these developments are updated at all times.

The Security and Corporate Resilience department (or the area that comes to assume its functions) will evaluate, at least once a year, compliance with and the effectiveness of this Policy.

Additionally, to verify compliance with this Policy, periodic audits will be carried out with internal or external auditors.

* * *

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 October 16th, 2025.