

Personal Data Protection Policy

Updated on October 13, 2026

The Board of Directors of NEOENERGIA S.A. (the “**Company**”) is empowered to continuously develop, assess and review the Company’s Governance and Sustainability System, as well as to approve and update the policies containing the guidelines governing the Company’s activities. Such policies also inform, where applicable, the policies that the companies within the group whose parent entity, as defined by law, is the Company may approve in the exercise of their corporate autonomy (the “**Subsidiaries**” and the “**Neoenergia Group**”).

In the exercise of these powers and within the framework of applicable law, the Company’s *Bylaws* and the *Purpose and Values of the Iberdrola Group* (“**Purpose and Values**”), the Board of Directors approves this *Personal Data Protection Policy* (the “**Policy**”), which respects, develops and adapts to the Company the *Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group* (the “**Ethical and Basic Principles of Governance and Sustainability**” and the “**Group**”, respectively).

1. Scope of Application

This Policy applies to the Company. Nevertheless, it includes principles that supplement the *Ethical and Basic Principles of Governance and Sustainability* with respect to personal data protection. Accordingly, the principles of this *Policy* inform the actions and specific regulations of the Subsidiaries, subject to their respective powers and autonomy in this area.

These principles shall also guide, where applicable, the activities of foundations affiliated with the Neoenergia Group.

The Company shall promote the alignment of the regulations of companies in which it holds an interest but which are not part of the Neoenergia Group, as well as those of joint ventures, temporary business associations and other entities under its management, with the personal data protection principles set forth in this *Policy*, and shall seek safeguards equivalent to those provided herein and under applicable regulations.

2. Purpose

The purpose of this *Policy* is to establish the principles governing the activities of the Company, as the Group’s subholding company in Brazil, and its Subsidiaries in matters of personal data protection, ensuring compliance with applicable regulations in all cases.

In particular, the *Policy* safeguards the right to protection of the data of natural persons who

interact with the Company, ensuring respect for the rights to honor and privacy in the processing of different types of personal data obtained from different sources and for purposes that vary according to its business activities, all in compliance with the Company's *Human Rights Respect Policy*.

3. Principles of Conduct

The Company adopts and promotes the following core principles of conduct, which shall form part of its personal data protection activities:

Principles of legitimacy, lawfulness and fairness in personal data processing:

Personal data shall be processed fairly, legitimately and lawfully in accordance with applicable regulations. Accordingly, personal data shall be collected for one or more specific and legitimate purposes consistent with applicable regulations.

Where required by applicable regulations, the consent of data subjects shall be obtained before their data is collected. Likewise, where required by law, the purposes of personal data processing shall be explicit and specified at the time of collection.

In particular, the Company shall not request or process personal data concerning ethnic or racial origin, political opinions, beliefs, religious or philosophical convictions, sexual life or orientation, trade union membership or health, nor genetic or biometric data intended to uniquely identify an individual, unless the collection of such data is necessary, legitimate and required or permitted by applicable regulations, in which case it shall be requested and processed in accordance therewith.

b) Principle of data minimization:

Only personal data that is strictly necessary for the purpose for which it is collected or processed, and appropriate to that purpose, shall be processed.

c) Principle of accuracy:

Personal data shall be accurate and kept up to date. Otherwise, it shall be deleted or rectified.

d) Principle of storage limitation:

Personal data shall not be retained beyond the period necessary to achieve the purpose for which it is intended, except as otherwise provided by law.

e) Principles of integrity and confidentiality:

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

Personal data requested and processed by the Company shall be maintained under the strictest confidentiality and shall not be used for purposes other than those that justified and permitted its collection, nor disclosed or transferred to third parties except as permitted by applicable regulations.

The Company shall maintain appropriate technical and organizational measures to ensure a level of security proportionate to the risk.

f) Principle of proactive accountability:

The Company shall be responsible for complying with the principles set forth in this *Policy* and with those required by applicable regulations, and shall be able to demonstrate such compliance when required by applicable law.

The Company shall assess the risks associated with its processing activities in order to determine the measures required to ensure that personal data is processed in accordance with legal requirements. Where required by law, the risks that new products, services or information systems may pose to personal data protection shall be assessed in advance, and the measures necessary to eliminate or mitigate such risks shall be adopted.

The Company shall maintain records of processing activities describing the personal data processing carried out in the course of its activities.

If an incident results in the accidental or unlawful destruction, loss or alteration of personal data, or in unauthorized disclosure of or access to such data, the internal protocols established by the Corporate Security and Resilience Department (or the area performing its functions from time to time), through the Security, Resilience and Digital Technologies Committee (or the committee performing its functions from time to time), and applicable law shall be observed. The Company shall document such incidents and adopt measures to address and mitigate any adverse effects on data subjects.

The Company shall appoint a Data Protection Officer (DPO) to ensure compliance with personal data protection regulations.

g) Principles of transparency and information:

Personal data processing shall be transparent to the data subject, and information regarding the processing of their data shall be provided in a clear and accessible manner where required by applicable law.

To ensure fair and transparent processing, the Company shall inform the affected persons or data subjects whose data it intends to collect of the circumstances relating to the processing, in accordance with applicable regulations.

The Company shall make accessible mechanisms available to data subjects to exercise their rights and submit inquiries or complaints relating to personal data protection.

h) Acquisition or obtaining of personal data:

The acquisition or obtaining of personal data from illegitimate sources, from sources that do not provide sufficient assurance of lawful provenance, or from sources whose data has been collected or transferred in violation of the law is prohibited.

i) Engagement of data processors:

Before engaging any service provider that will access personal data under the Company's control, and throughout the contractual relationship, the Company shall adopt the measures necessary to ensure and, where legally required, demonstrate that the processor's data processing complies with applicable law. In particular, the Company shall require processors to maintain a level of protection equivalent to and consistent with this Policy.

j) International data transfers:

Any processing of personal data subject to the regulations of the ANPD – Brazilian Data Protection Authority that involves a transfer of data outside Brazil shall be carried out in strict compliance with the requirements established by the applicable law of the jurisdiction of origin.

k) Rights of data subjects:

The Company shall enable data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability and objection that apply in each jurisdiction, establishing the internal procedures required to satisfy at least the legal requirements applicable in each case.

The Company shall establish clear and accessible procedures for submitting requests or complaints relating to personal data protection.

The Company shall ensure that these core principles of conduct are observed by third parties that access personal data for which the Company is responsible, through measures and safeguards equivalent to those provided under this Policy and applicable regulations.

4. Group-Level Coordination

The Security and Resilience Department, through the Security, Resilience and Digital Technologies Committee (or the committee or department performing its functions from time to time), shall ensure appropriate coordination within Neoenergia of personal data protection practices and risk management, and shall establish appropriate coordination procedures with the security, resilience and digital technologies committees or security departments (or the committee or department performing their functions from time to time) of the subholding companies.

The Legal Services departments in each country shall be responsible for reporting to the Security, Resilience and Digital Technologies Committee (or the committee performing its functions from time to time) on regulatory developments and updates in the field of personal data protection.

In addition, the business units and corporate departments shall: (i) appoint the persons responsible for data, who shall act in coordination and under the supervision of the Security, Resilience and Digital Technologies Committee (or the committee performing its functions from time to time) and the Security and Resilience Department (or the department performing its functions from time to time); and (ii) coordinate with the Security and Resilience Department (or the department performing its functions from time to time) any activity that entails or involves the processing of personal data, while respecting in all cases the special framework of enhanced autonomy applicable to listed subholding companies within the Group.

5. Implementation and Monitoring

For the implementation and monitoring of this Policy, the Board of Directors is supported by the Security and Resilience Department (or the department performing its functions from time to time), which, through the Security, Resilience and Digital Technologies Committee (or the committee performing its functions from time to time), shall develop and keep up to date, in accordance with this Policy, the internal rules governing personal data protection management. Such rules shall be implemented by the Security and Resilience Department and shall be mandatory for members of the management team and the Company's professionals.

Without prejudice to the foregoing, the Company's Systems Department (or the department

performing its functions from time to time) shall be responsible for ensuring the proper implementation of the Company's information systems and the IT controls and developments required to ensure compliance with internal data protection regulations, and for keeping such developments current at all times.

The Security and Resilience Department (or the department performing its functions from time to time) shall review and assess, at least annually, compliance with and the effectiveness of this Policy, including to ensure its continued alignment with applicable regulations.

Periodic audits shall be conducted by internal or external auditors to verify compliance with this Policy.

* * *

This Policy was initially approved by the Board of Directors on June 28, 2018 and was most recently updated at the Board of Directors' Meeting held on October 13, 2026.