Personal Data Protection Policy

25 March 2025

The Board of Directors of IBERDROLA, S.A. (the "**Company**") has the power to design, assess and continuously revise the Governance and Sustainability System, and specifically to approve and update policies, which contain the guidelines governing the conduct of the Company, and furthermore, to the extent applicable, that inform the policies that the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the "**Group**"), decide to approve in the exercise of their autonomy.

In exercising these powers and within the framework of legal regulations, the By-Laws and the Purpose and Values of the Iberdrola Group, the Board of Directors hereby approves this Personal Data Protection Policy (the "**Policy**"), which respects, further develops and adapts the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group with respect to the Company.

1. Scope of Application

This Policy applies to the Company. Without prejudice to the foregoing, it includes basic principles that, in the area of personal data protection, complement those contained in the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group and, to this extent, must inform the conduct and standards-setting implemented by the other companies of the Group in this area in the exercise of their powers and in accordance with their autonomy.

To the extent that listed country subholding companies form part of the Group, they and their subsidiaries, under their own special framework of enhanced autonomy, may establish principles and rules that must have content consistent with the principles of this Policy.

To the extent applicable, these principles must also inform the conduct of the foundations linked to the Group.

For companies that do not form part of the Group but in which the Company holds an interest, as well as for *joint ventures*, temporary *joint ventures* (*uniones temporales de empresa*) and other entities in which it assumes management, the Company shall also promote the alignment of its regulations with the basic principles regarding personal data protection contained in this Policy.

2. Purpose

The purpose of this Policy is to establish the main principles of conduct that are to govern the Company as regards personal data protection, ensuring compliance with applicable legal provisions under all circumstances.

In particular, this Policy guarantees the right to the protection of personal data for all natural persons who establish relations with the Company, 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 in compliance with the Company's Policy on Respect for Human Rights.

3. Main Principles of Conduct

The Company adopts and promotes the following main principles of conduct that must inform all of its activities in the area of personal data protection:

a. Principle of legitimate, lawful and fair processing of personal data.

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

   When so required by applicable legal provisions, the consent of the data subjects must be obtained before their data are collected.

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

In particular, the Company shall not collect 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 legal provisions, in which case they shall be collected and processed in accordance with the provisions thereof.

b. Principle of minimisation.

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

c. Principle of accuracy.

Personal data must be accurate and up-to-date. They must otherwise be erased or rectified.

d. Principle of storage duration limitation.

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

e. Principles of integrity and confidentiality.

Personal data must be processed in a manner that uses technical or organisational measures to ensure appropriate security that protects the data against unauthorised or unlawful processing and against loss, destruction or accidental damage.

The personal data collected and processed by the Company must 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 other than in the cases permitted by applicable legal provisions.

f. Principle of proactive responsibility (accountability).

The Company shall be responsible for complying with the principles set forth in this Policy and with those required by applicable legal provisions and must be able to demonstrate compliance when so required by applicable legal provisions.

The Company must perform a risk assessment of the processing that it carries out in order to identify the measures to apply to ensure that personal data are processed in accordance with legal requirements. When so required by legal provisions, it shall perform a prior assessment of the risks that new products, services or IT systems may involve for personal data protection and shall adopt the necessary measures to eliminate or mitigate them.

The Company must maintain a record of activities in which they describe the personal data processing that it carries out in the course of its activities.

In the event of an incident causing the accidental or unlawful destruction, loss or alteration of personal data, or the disclosure of or unauthorised access to such data, the Company must follow the internal protocols established for such purpose by the Company's Security and Resilience Division (or by such division as assumes the powers thereof at any time) through the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) and those that are established by applicable legal provisions. The Company must document such incidents and shall adopt measures to resolve and mitigate potential adverse effects for data subjects.

The Company shall designate a data protection officer in order to ensure compliance with the legal provisions on personal data protection.

g. Principles of transparency and information.

Personal data shall be processed in a transparent manner in relation to data subjects, with the provision to data subjects of intelligible and accessible information regarding the processing of their data when so required by applicable law.

For purposes of ensuring fair and transparent processing, the Company must inform data subjects whose data are to be collected of the circumstances relating to the processing in accordance with applicable legal provisions.

h. Acquisition or procurement of personal data.

It is forbidden to purchase or obtain personal data from unlawful sources, from sources that do not sufficiently ensure the lawful origin of such data or from sources whose data have 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 the Company is responsible, as well as during the effective term of the contractual relationship, the Company must adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing by the data processor is performed in accordance 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 must be carried out strictly in compliance with the requirements established by applicable law in the jurisdiction of origin.

k. Rights of data subjects.

The Company must allow data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability and objection that are applicable in each jurisdiction, establishing for such purpose such internal procedures as may be necessary to at least satisfy the legal requirements applicable in each case.

4. Group-level Coordination

The Security and Resilience Division, through the Security, Resilience and Digital Technology Committee (or such committee or division as assumes the powers thereof at any time), shall ensure appropriate Group-level coordination of the practices and management of risks in the area of personal data protection and shall establish appropriate coordination procedures with the security, resilience and digital technology committees or with the security divisions (or such committee or division as assumes the powers thereof at any time) of the country subholding companies.

The Legal Services divisions of each country shall be responsible for reporting to the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) regulatory developments and news that occur in the area of personal data protection.

In addition, the businesses and corporate divisions must (i) appoint the persons responsible for the data, who shall act on a coordinated basis and under the supervision of the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) and of the Security and Resilience Division (or such division as assumes the powers thereof at any time); and (ii) coordinate with the Security and Resilience Division (or

such division as assumes the powers thereof at any time) any activity that involves or entails the management of personal data, in all cases adhering to the special framework of strengthened autonomy of the listed country subholding companies.

5. Implementation and Monitoring

For the implementation and monitoring of the provisions of this Policy, the Board of Directors is assisted by the Security and Resilience Division (or such division as assumes the powers thereof at any time), which, through the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time), shall develop and keep updated, in accordance with the provisions of this Policy, the internal regulations for the management of personal data protection, which shall be implemented by the Security and Resilience Division and which shall be mandatory for the members of the management team and the professionals of the Company.

Without prejudice to the foregoing, the Company's Systems Division (or such division as assumes the powers thereof at any time) shall be responsible for ensuring the proper implementation of the information technology systems of the Company, the information technology controls and developments that are appropriate to ensure compliance with the internal data protection rules and that said developments are updated at all times.

The Security and Resilience Division (or such division as assumes the powers thereof at any time) shall evaluate compliance with and the effectiveness of this Policy.

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

* * *

This Policy was initially approved by the Board of Directors on 21 July 2015 and was last amended on 25 March 2025.