15. Personal Data Protection Policy

DS C

18 December 2018

Index

The Board of Directors of IBERDROLA, S.A. (the "**Company**") is responsible for formulating the strategy and approving the *Corporate Policies* of the Company, as well as for organising the internal control systems. In fulfilling these responsibilities, and in order to lay down the general principles that are to govern the processing of personal data at all of the companies belonging to the group of which the Company is the controlling company, within the meaning established by law (the "**Group**"), the Board of Directors approves this *Personal Data Protection Policy*.

1. Purpose

This *Personal Data Protection Policy* establishes the common principles and guidelines for conduct that are to govern the Group as regards personal data protection, ensuring compliance with applicable law under all circumstances.

In particular, the *Personal Data Protection Policy* is intended to guarantee the right to protection of personal data for all natural persons who establish relations with the companies belonging to 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.

2. Scope

The *Personal Data Protection Policy* shall apply to the Company, to the other companies within the Group, to the directors, officers and employees thereof, and to all persons who establish relations with companies belonging to the Group.

By way of exception to the foregoing, both listed country subholding companies and unlisted companies that are not wholly-owned by the Group that have their own personal data protection policy, as well as the respective subsidiaries thereof, shall not be covered by this *Personal Data Protection Policy*. Without prejudice to the foregoing, in both cases, the policies of these companies shall provide the mechanisms required to ensure proper coordination with the rest of the Group in the area of personal data protection.

At those companies or entities in which the Company has a direct or indirect interest but that do not form part of the Group, the representatives thereof shall procure compliance with the provisions of this *Personal Data Protection Policy* and, to the extent possible, shall promote the application of the principles thereof.

3. Principles for the Processing of Personal Data

The principles underpinning the *Personal Data Protection Policy* are as follows:

a) General principles:

Group companies shall thoroughly comply with personal data protection law in their jurisdiction, the laws that apply based on the processing of personal data that is carried out and the laws determined by binding rules or resolutions adopted within the Group.

Group companies shall strive to ensure that the principles set forth in this *Personal Data Protection Policy* are taken into account (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 contracts and obligations that they formalize with natural persons, and (iv) in the implementation of any systems and platforms that allow access by employees or third parties to personal data and/or the collection or processing of such data.

b) Principles relating to the processing of personal data.

(i) *Principle of legitimate, lawful and fair processing of personal data.*

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

When so required by law, the consent of the data subjects must be obtained before their data are 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.

In particular, Group companies 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 law, in which case they shall be collected and processed in accordance with the provisions thereof.

(ii) *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.

(iii) *Principle of accuracy.*

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

(iv) *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.

(v) *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 accidental loss, destruction or damage.

The personal data collected and processed by Group companies 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 law.

(vi) *Principle of proactive responsibility (accountability).*
Group companies shall be responsible for complying with the principles set forth in this *Personal Data Protection Policy* and those required by applicable law and must be able to demonstrate compliance when so required by applicable law.
Group companies must perform a risk assessment of the processing that they carry 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 law, they shall perform a prior assessment of the risks that new products, services or IT systems may imply for personal data protection and shall adopt the necessary measures to eliminate or mitigate them.
Group companies must maintain a record of activities in which they describe the personal data processing that they carry out in the course of their 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 internal protocols established for such purpose by the Corporate Security Division and those that are established by applicable law must be followed. Such incidents must 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 shall be designated in order to ensure that Group companies comply with the legal provisions on data protection.

(vii) *Principles of transparency and information.*
Personal data shall be processed in a transparent manner with 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 Group company that is responsible for the processing must inform data subjects whose data is to be collected of the circumstances relating to the processing in accordance with applicable law.

(viii) *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.

(ix) *Engagement of data processors.*
Prior to engaging any service provider that may have access to personal data for which Group companies are responsible, as well as during the effective term of the contractual relationship, such Group companies must adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing by service provider is performed in accordance with applicable law.

(x) *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. In addition, Group companies located outside the European Union must comply with any requirements for international transfers of personal data that are applicable in their respective jurisdictions.

(xi) *Rights of data subjects.*
Group companies 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. Implementation

In accordance with the provisions of this *Personal Data Protection Policy*, the Corporate Security Division, together with the Legal Services of the Company, shall develop and keep updated internal rules for global data protection management at the Group level, which shall be implemented by the Corporate Security Division and which shall be mandatory for all officers and employees at the Company.
Likewise, the Corporate Security Division and the Legal Services Division of each country, or such divisions as may assume the duties thereof, shall establish local internal procedures designed to implement the principles laid down in this *Personal Data Protection Policy* and to adapt the content thereof in accordance with applicable law in their respective jurisdictions.
The Legal Services Division shall be responsible for informing the Corporate Security Division of regulatory developments and news that occur in this area.
The Systems Division, or such division as may assume the duties thereof, shall be responsible for implementing the information technology systems of the companies of the Group, 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 must (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 Corporate Security Division; and (ii) coordinate with the Corporate Security Division 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 and any particular provisions that might be established at those unlisted country subholding companies that are not wholly owned by the Group.
Finally, the Cybersecurity Committee, created pursuant to the provisions of the *Cybersecurity Risk Policy*, shall monitor the general status of personal data protection at companies of the Group and shall endeavour to ensure proper Group-level coordination of

risk practices and management in the area of personal data protection, assisting the Corporate Security Division in the approval of internal rules in this area.

5. Control and Evaluation

a) Control
   The Corporate Security Division, or the division assuming the duties thereof, shall supervise compliance with the provisions of this *Personal Data Protection Policy* by the Company and the other companies of the Group. The foregoing shall in any event be without prejudice to the responsibilities vested in other bodies and divisions of the Company and, if applicable, in the management decision-making bodies of the other companies within the Group.
   Regular audits shall be performed with internal or external auditors in order to verify compliance with this *Personal Data Protection Policy*.

b) Evaluation
   The Corporate Security Division shall evaluate compliance with and the effectiveness of this *Personal Data Protection Policy* at least once per year and shall report to the Finance and Resources Division, or to the division assuming such duties at any particular time, on the results of such evaluation.

This *Personal Data Protection Policy* was initially approved by the Board of Directors on 15 December 2015 and was last amended on 18 December 2018.