Binding corporate rules of the Iberdrola Group

December 2020

www.iberdrola.com

IBERDROLA

Index

INTRODUCTION

The Binding Corporate Rules (hereinafter referred to as "**BCRs**") express the global commitment of all the companies which compose the Iberdrola Group bonded to these BCRs (Iberdrola, S.A. a controlling company and each of its controlled undertakings which are also bonded to these BCRs, hereinafter "**Iberdrola Group**" and each of its bonded companies, the "**Group Companies**") with privacy and data protection and establish the framework of appropriate guarantees for the transfer and the processing of personal data between them.

These BCRs are adopted in line with the provisions included in the Regulation (UE) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/CE (hereinafter referred to as "**GDPR**").

These BCRs apply to all personal data, processed within the European Economic Area (hereinafter, the "EEA"), by Group Companies acting as data controller or as data processor acting on behalf of a data controller part of the Group, and transferred directly or indirectly from Group Companies located in the EEA to Group Companies located out of the EEA, and related to candidates, employees, suppliers, volunteers, event attendees and participants in master's degree scholarships competitions and beneficiaries thereof.

The obligations stated in these BCR's apply to Group Companies acting as Data Controllers and also to Group Companies acting as internal Data Processors.

By adhering to these BCRs, Group Companies undertake to respect them and comply with their provisions in the collection, compilation and processing of personal data for the fulfilment of their own purposes, and to enforce them for all their employees.

The Global Corporate Security Data Protection Coordinator will ensure that Group Companies comply with these BCRs in a coordinated manner and according to common interpretative criteria.

These BCRs and the Group Companies are published on www.iberdrola.com, and on the Intranet of the Iberdrola Group.

1. DEFINITIONS

a) "**Personal Data**": any information relating to an identified or identifiable natural person ("data subject");

   As an example, the following are considered personal data: name, address, social security number, driving license number, bank account number, family information, e-mail account address or vocational training.

   Special categories of personal data are ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data allowing the unambiguous identification of an individual, data relating to health, life and sexual orientation.

b) "**Processing**": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

c) "**Data controller**": natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing.

   In these BCRs, the Data Controller will be the Group Company that transfers personal data, and the Group Company receiving the data when the Company processes the data for its own purposes.

d) "**Data processor**": natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

   For the purposes of these BCRs, the Data processor shall also be the Group Company providing services in accordance with the corresponding contract for the provision of services.

e) "**Recipient**": natural or legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not.

f) "**Third party**": natural or legal person, public authority, agency or body other than the data subject, data controller, data processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

g) "**Iberdrola Group or Group**": a group constituted by Iberdrola, S.A. the controlling company and its controlled undertakings.

h) "**Group Companies**": each of the Iberdrola Group companies which are bonded to the BCRs, through the conclusion of the Intra-group Agreement on BCRs.

i) "Parent Company": according to the Spanish Commercial Code, in the Iberdrola Group, the parent company is the Group Company that meets any of the requirements in relation to the other subsidiary companies:

   1. It holds the majority of the voting rights.
   2. It has the power to appoint or dismiss the majority of the members of the governing body.
   3. It can avail of the majority of the voting rights by virtue of agreements held with third parties.
   4. It has exclusively assigned its voting rights to the majority of the members of the governing body, who are in office at the time of the preparation of the consolidated accounts and during the two years immediately prior thereto.

j) "**Subholding Company**": a company that groups together in Spain, the United Kingdom, the United States, Mexico and Brazil the Iberdrola Group companies domiciled in those countries that do not depend directly on Iberdrola, S.A., but on the subholding of the corresponding country. Exceptionally, Iberdrola Energía Internacional, S.A. groups together the Iberdrola Group companies which do not depend on any of the subholding companies of the aforementioned countries nor do they directly depend on Iberdrola, S.A. The Subholding Company depends directly on Iberdrola, S.A. and, therefore, its subsidiaries companies form part of the Iberdrola Group.

k) "**Binding Corporate Rules**": personal data protection policies which are adhered to by a Group Company established on the territory of a Member State for transfers or a set of transfers of personal data to a Group Company in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

l) "**Supervisory authority**": an independent public authority which is established by a Member State to monitor and ensure consistent application of the GDPR.

m) "**Spanish Data Protection Agency**": Supervisory Authority competent to monitor and coordinate the authorization procedure of the BCR, to approve them and to inform the Supervisory Authorities concerned about any update of the BCR or of the list of members of the BCR.

n) "**Data subject**": the person to whom the personal data being transferred from the EEA to third countries belongs.

o) "**Data exporter**": A Group Company established in an EEA country, which transfers personal data directly or indirectly to another Group Company not established in a in an EEA country.

p) "**Data importer**": A Group Company which is not established in an EEA country and receives personal data from a data exporter.

q) "**Security measures**": appropriate technical and organizational measures that ensure a level of security appropriate to the risk.

r) "**Consent**": any freely given, specific, informed and unambiguous indication by which the data subject accepts, by a statement or by a clear affirmative action, the processing of personal data relating to him or her.

s) "**Third country**": a country other than the EU member states and the EEA countries.

t) "**Member state law**": refers to an EU member state national law, and the EEA countries law.

On all matters not covered in this section, Group Companies shall understand these BCRs in accordance with GDPR.

2. SCOPE OF APPLICATION

2.1. BCRs MATERIAL SCOPE OF APPLICATION

The BCRs cover the following processing of personal data:

- **Candidates for a job in the Iberdrola Group:** Identifying and curricular data about candidates for a job or internship, which register in the Iberdrola Group employment portal, in order to allow its participation in possible recruitment for staff or student interns processes. His or her personal data may be transferred to any Company of the Group, even outside the EEA, that has an interest in his or her profile, leading to an international transfer of data.
- **Employees:** Personal data of employees obtained as a consequence of the employment relationship, in the process of formalising the relationship and during the period in which it is maintained. These data may be communicated to Group companies, including those outside the EEA, for internal filling of vacancies, for the management of the employment relationship, in compliance with service contracts and for the management and organisation of teams. All these international transfers are necessary for the management and fulfilment of the employment relationship with the employee.
- **Suppliers:** Identifying data, personal and professional characteristics, commercial information, economic data and data relating to transactions of goods and services of suppliers, all with the aim of carrying out a global management of suppliers. These data are communicated to the Group companies, including those outside the EEA. The international transfer is carried out as a consequence of the use of a common database for all companies of the Iberdrola Group.
- **Volunteers**: Identifying data from volunteers for the management of Iberdrola's volunteer programme and related activities. These data are communicated to Iberdrola Group Companies, including those outside the EEA, that offer a volunteer action. The international transfer is carried out by Iberdrola, S.A., which is responsible for processing the Iberdrola Group's personal volunteer data included in a global file, and by other Group Companies established in the EEA, which are responsible for processing the volunteer data.
- **Event Attendees:** Identifying data from event attendees in order to manage corporate events. These data will be communicated to other companies of the Iberdrola Group for internal administrative purposes. The international transfer is carried out by Iberdrola, S.A. and by other Group Companies established in the EEA as data controllers of the processing of the event attendee's data.
- **Participants in master's degree scholarships competitions and beneficiaries thereof:** Identifying, academic and professional data of participants in applications for master's degree scholarships: in order to manage and award the scholarships. The information provided by the applicant is incorporated into a database to which the subholding company of the Group that calls the scholarship for which the application has been made will have access. Iberdrola, S.A. also has access to this personal data as the entity in charge of the overall internal administrative management of the Iberdrola Group's scholarships.

2.2. BCRs GEOGRAPHICAL SCOPE OF APPLICATION

These BCRs apply to the transfers and personal data processing of candidates, employees, suppliers, volunteers, event attendees and participants in master's degree scholarships competitions and beneficiaries thereof, carried out by Group Companies acting as Data controllers or Data processors. Therefore, these BCRs apply to the Group Company established in an EEA country exporting personal data directly or indirectly, and to the Group Company not established in an EEA country importing the personal data.

The BCRs apply to first transfers of personal data and to the onward transfers.

These BCRs are binding on the Group Companies which have signed the Intra-group Agreement on BCR ("IA") expressing their acceptance with a declaration which is included as an annex to the said agreement. Likewise, Annex I of these BCRs includes a list of the Group Companies which are bonded to these BCRs, grouped by the Group Companies that directly or indirectly have control over the first ones. In case of doubts related to the Group Com-

panies bonded to these BCRs, please contact the Global Corporate Security Data Protection Coordinator, whose contact details are: dpo@iberdrola.com

Under GDPR and applicable labour legislation, these BCRs are binding and enforceable on the Iberdrola Group employees of all the Group companies. Employees have been informed of its existence, indicating that they are mandatory and establishing that, according with the applicable legislation and the corresponding employment contract of each of the Group Companies, they corresponding disciplinary regime shall be applied, in case of non-compliance.

The processing activities and the categories of personal data within the scope of the BCRs are those related to candidates, employees, suppliers, volunteers, event attendees and participants in master's degree scholarships competitions and beneficiaries thereof are subject to the BCRs, which shall apply to both manual and automated processing. The personal data transfers are carried out among Group Companies during their usual business activities and such data can be stored in centralized data bases, that can be accessed by Group Companies from any part of the world where Iberdrola Group is established.

3. PRINCIPLES

Any personal data processing carried out by Group Companies, either as Data controller or Data processor, shall comply will the following principles, that are implemented through corporate rules, procedures, methodologies and tools of the Iberdrola Group.

3.1. COMPLIANCE WITH LOCAL LEGISLATION AND THE GDPR

In addition to comply with these BCRs, each Group Company shall comply with applicable local legislation related to personal data, and shall ensure that the collection and use of personal data is carried out in accordance with it.

3.2. LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The processing of the data will be lawful if it's based on any of the following conditions established in the GPDR:

a. **Consent:** the data subject has consented to the processing of his or her personal data for one or several specific purposes. For example, the processing of employees' images by Group Companies for social and corporate communication purposes is carried out if the data subject has given his or her consent.

   If consent is the lawful basis for processing, the Data controller shall ensure that it has been obtained:

   1. **Freely**: in order for consent to be free, there must be a real choice by the data subject for not giving it.
   2. **Specific**: the purposes of the processing must be specific and cannot be blurred or expanded once the data subject has consented to the collection of his or her data.
   3. **Informed:** it is necessary for the Controller to inform the data subject about the purposes of the processing and shall be obliged to enlarge on that information, where necessary, to guarantee the data subject really understands the processing operations.
   4. **Unequivocal:** consent shall be referred to each specific processing of personal data.

   Consent must be obtained independently from the acceptance of any type of clause related to the terms and conditions of the legal relationship on which it is based and using a clear and simple language.

   A record of when and how the consent was obtained from the data subject shall be kept and for what specific purpose, as well as the documentary basis thereof.

   Furthermore, the data controller shall guarantee that the data subject may withdraw his or her consent at any time in a manner as easy as giving it.

b. **Contractual relationship:** the processing is necessary for performance of a contractual relationship between the Group Company and the data subject or for the application of pre-contractual measures requested by the data subject.

c. **Legal Obligation**: the processing is necessary to ensure that the Group Company, acting as data controller or processor, complies with a legal obligation.

d. **Vital Interest:** the processing is necessary to protect the vital interests of the data subject or another natural person.

e. **Public Interest:** the processing is necessary to ensure the Controller fulfils a mission of public interest.

f. **Legitimate Interest:** the processing is necessary for the satisfaction of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Data subjects must be informed about the processing activities done with their personal data. In particular, it should be informed about:

a. The identity and contact details of the Controller and, where applicable, of the controller's representative.

b. The contact details of the Data Protection Officer.

c. The purposes of the processing.

d. The legal basis for the processing. When the legal basis is the legitimate interest pursued by the Data Controller or by a third party, as long as such interest isn't overridden by the interests or the fundamental rights and freedoms of the data subject, it must be informed about this legitimate interest.

e. The categories of personal data concerned.

f. Data retention periods or the criteria used to determine them.

g. The existence of automated decisions or profiling.

h. If there's any third-party disclosure, the recipients or categories of recipients shall be indicated.

i. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of not providing such data.

j. Whether or not there is an intention to make international data transfers to third countries and if so, the protection guarantees that will apply to them.

k. Data protection rights of the data subjects. These are: right of access, right to rectification and erasure, restriction of processing, right to object to processing and right to data portability. Where processing is based on (i) the consent of the data subject for one or more purposes or (ii) explicit consent to the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health or data concerning a natural person's sex life or sexual orientation, the right to withdraw consent shall be informed at any time.

l. Right to lodge a complaint with a Supervisory Authority, in case the data subject considers its right to the protection of personal data, provided by the regulation applicable and these BCRs, hasn't been guaranteed.

m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

n. Where the controller intends to further process the personal data for a purpose other than that for which personal data were initially collected, the controller shall provide the data subject prior to that further processing with information on that purpose and with any relevant information in accordance with the preceding paragraphs.

o. In the event that data are not directly obtained from the data subject, in addition to that indicated in the previous sections, the source from which the personal data originates and where appropriate, whether they come from publicly accessible sources must be indicated.

3.3. PURPOSE LIMITATION

Personal data shall be collected for specific, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes other than those originally established. For example, the signing up of a supplier only requires the information necessary in order to maintain and manage the business relationship (general identification and contact data, banking and transactional data such as invoices and contracts) and is only processed for that purpose, and will not be process for the purposes for which it is not intended to be used.

3.4. DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes of the processing. Only information that is strictly necessary for the purposes of the processing should be collected. Specifically, each Group company has access to the full details of its suppliers, and access by the other Group companies is restricted to general supplier details only (identification, contact and banking details).

3.5. ACCURACY

Personal data must be accurate and be kept updated. Particularly,

a. All the information repositories, including applications, databases, spread sheets, etc. shall include, when possible, a data validation mechanism to ensure the information is accurate and complete.

b. Periodic review and continuous improvement processes shall be established with respect to the information to verify that the data is accurate and up to date.

3.6. STORAGE PERIOD LIMITATION

Personal data shall be stored in such a way as to enable the identification of the data subjects for no longer than necessary for the purposes of the processing. In particular:

a. All personal data processing must have an established retention periods included in the Record of Processing Activities, which shall be implemented through a manual or automated process.

b. Personal data cannot be stored for longer than the period established through manual or automated process.

c. Those retention periods established by legislation, standards or other applicable regulation, both national and sectoral, in each case, shall be considered mandatory. Without prejudice of blocking the data when the processing for which they were collected has ended.

3.7. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The Group Companies are prohibited from processing special categories of personal data, unless:

a. **The Data subject has given explicit consent** to the processing of those special categories of personal data for one or more specified purposes, and such consent is considered as valid pursuant to the applicable law and regulation;

b. **The Processing is necessary for the purpose(s) of carrying out the obligations and exercising specific rights** of the Controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by applicable law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. **The processing is necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving his consent;

d. **The processing relates to personal data** which has been manifestly made public by the data subject;

e. **The processing is necessary for the establishment, exercise or defense of legal claims** or whenever courts are acting in their judicial capacity.

3.8. INTEGRITY AND CONFIDENTIALITY

Personal data is processed in such a way as to guarantee the appropriate security thereof, applying the appropriate technical and organisational measures.

To guarantee this principle, the personal data for which a Group Company is controller or processor shall be processed:

a. Securely and protected against unauthorized or illegal processing and against accidental or unlawful destruction, loss or alteration. To this end, the security measures considered necessary will be implemented in each case in accordance with the level of risk of the processing activity in question.

b. Under conditions that ensure the permanent confidentiality, integrity, availability and resilience of the processing systems and services.

c. Under conditions that guarantee the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident.

The technical and organisational measures developed and implemented to guarantee the security of the personal data and its processing shall be subject to regular verification, assessment and evaluation of their effectiveness.

The Group Companies shall respect the *Iberdrola Group Cybersecurity Framework*, which defines the program, policies, standards and processes necessary to manage cybersecurity risks in Iberdrola's operating environment.

3.9. PERSONAL DATA BREACHES

If there is any Security breach that causes the accidental or illegal destruction, loss or alteration of personal data, as well as any unauthorized communication or access to personal data transmitted, stored or processed in some other way, the Group Company, Data Controller or Processor, shall follow the internal procedure of Iberdrola Group: *Data protection incidents response procedure,* that determines the organisation and performance criteria for the detection, containment, risk assessment, communication and notification of security breaches in which personal data are involved.

This procedure establishes the obligation of the Group Companies that have been affected by a Personal Data Breach related to personal data transferred from the EEA, to notify, without undue delay, to the Group Companies that accept responsibility for any violation of the BCRs by any of the Group Companies established outside the EEA, and to the Global Corporate Security Data Protection Coordinator.

In the event that the Personal Data Breach is likely to result in a risk to the rights and freedoms of the data subjects, the Local Corporate Security Data Protection Coordinator, or as the case may be, the Global Corporate Security Data Protection Coordinator will notify the competent Supervisory Authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the data subjects, the affected Companies shall communicate it directly to the data subject without undue delay.

The Personal Data Breach notifications must be documented and shall at least:

a. Describe the nature of the Personal Data Breach: number of data subjects concerned, categories of data subjects concerned, approximate number of personal data records concerned, etc.

b. Name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

c. The likely consequences and effects of the Personal Data Breach;

d. Describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

This documentation shall be made available to the Spanish Data Protection Agency and any other Supervisory Authority upon request.

3.10. PROCESSING BY DATA PROCESSORS

Group Companies will not contract the services of a supplier who has access to personal data for which the Company is Data Controller, without first ensuring that the data processor will implement appropriate technical and organisational measures to ensure the protection of the rights and freedoms of data subjects.

A contract or other similar legal act must be signed that binds the Processor to the Controller and establishes the object, duration, nature and purpose of the processing, the type of personal data and the categories of data subjects to which they refer, the rights and obligations of the Controller and of the Processor. The following shall be minimum obligations of the Processor, and expressly provided for in the contract or similar legal act:

a. Process personal data only on the basis of documented instructions from the Data controller, including transfers of personal data to a third country or an international organisation, unless obliged to do so by virtue of EU or Member State law which applies to the Processor.

   In such case, and unless prohibited by such law for reasons of public interest, the Processor shall inform the Controller of such legal requirement prior to the processing.

b. Ensure that persons authorised to process personal data have committed to respect confidentiality or are subject to a statutory obligation of confidentiality.

c. Take all necessary measures to guarantee the security of the processing.

d. Access to the personal data by another Data processor will not be granted without the prior written, specific or general authorisation from the Controller. In any case, the data processing by the new sub-processor must comply with the instructions of the Controller, and the Data Processor must sign a contract with the new sub-processor in accordance with the provisions of article 28 of GDPR.

e. Assist the Controller, taking into account the nature of the processing, by means of appropriate technical and organisational measures, whenever possible, so that he can fulfil its obligation to respond to requests for the exercise of data subjects' rights.

f. Help the Data controller to guarantee the fulfilment of the obligations established in the GDPR, taking into account the nature of the processing and the information available to the Processor:

   - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
   - The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.
   - The Data Processor shall provide reasonable assistance to the Data Controller when carrying out any Data Protection Impact Assessment, and in prior consultations with Supervising Authorities or other competent Data Privacy Authorities, when appropriate.

g. At the choice of the Controller, erase or return all personal data once the provision of services has been completed, and erase existing copies unless the retention of personal data is required under EU or Member State law.

h. Make available to the Controller all the information necessary to demonstrate compliance with the Processor obligations, as well as to allow and contribute to the audits, including inspections, carried out by the Controller or any other authorized auditor.

i. Immediately inform the Controller in the event of non-compliance with its obligations as Data processor.

3.11. INTERNATIONAL PROCESSING OF PERSONAL DATA

Processing of personal data involving a transfer of data to Controllers and Processors who are not part of the Iberdrola Group and are located in countries outside the EEA should be subject to additional safeguards to ensure that the level of protection is adequate. Therefore, the transfer of personal data from a Group Company to Group Companies not adhered or to third companies can only take place:

1) When the countries in which the recipient companies (from the Group or third parties) are located offer an adequate level of protection, in accordance with an adequacy decision of the European Commission.

2) When the countries in which the recipient companies are located are not those of paragraph 1), the Data Controller or Data processor will take the appropriate measures to compensate for the lack of data protection in the country of destination. For example:

   - Standard contractual clauses for data protection adopted by the European Commission or by a supervisory authority;
   - Binding corporate rules from Data Processors;

- Binding codes of conduct, setting out the obligations of adhered companies regarding the international transfer of data in accordance with the GDPR; together with binding commitments of the controller or processor in the third country to apply appropriate safeguards, including as regards data subjects' rights.
- Personal data protection certification demonstrating that certified companies comply with the GDPR in relation to international transfers; together with binding commitments of the controller or processor in the third country to apply appropriate safeguards, including as regards data subjects' rights.
- Legally binding and enforceable instrument between public authorities or bodies.

Apart from the situations mentioned in the two previous sections, international data transfers may only be carried out by Group Companies to Group Companies not adhered or to third companies if:

- The data subject has provided explicit and informed consent.
- The international transfer is necessary for (i) the conclusion or execution of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (ii) it is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (iii) to protect a vital interest of the data subject or of other persons, when the data subject is physically or legally incapacitated to give consent; or (iv) it is necessary for the establishment, exercise or defence of legal claims.
- The international transfer has been authorised by the Supervisory Authority prior to its execution and on the basis of contractual clauses agreed between the Data controller or Data processor and the controller, processor or recipient of personal data in the third country.
- The international transfer is based on a legitimate interest of the Data Controller, when such interest isn't overridden by the interests or fundamental rights and freedoms of the data subject, and in addition it is (i) not repetitive, and (ii) affects a limited number of persons, and (iii) specific and appropriate data protection safeguards are adopted. It will also be necessary to inform the Supervisory Authority and the data subject. This situation is only admissible in exceptional circumstances and where none of the three previous reasons for the transfer are applicable.

The fact that the international transfer of data is the result of the provision of services does not exempt the data controller from the obligation to enter into a contract with the data processor in accordance with the provisions of the GDPR.

The Iberdrola Group's internal procedure denominated *Procedure for international transfers of personal data* establishes the guidelines to be followed in accordance with GDPR when a Group Company located in the EEA must carry out international transfers of personal data to recipients outside the EEA.

3.12. RECORD OF PROCESSING ACTIVITIES

Each Data Controller and Data Processor shall maintain a Record of Processing Activities, which shall be recorded in writing, including in electronic form, in which all the processing of personal data carried out shall be recorded. The Record of Processing Activities shall be made available to the supervisory authority on request.

The Record of Processing Activities shall contain:

a. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b. the purposes of the processing activities;

c. a description of the categories of data subjects and the categories of personal data;

d. the categories of recipients to whom the personal data are disclosed, including third country recipients;

e. where applicable, transfers of personal data to a third country, including the identification of such country or international organisation and, in the case of transfers referred to in clause 3.11;

f. the data retention periods of the different data categories;

g. a general description of the technical and organisational security measures implemented to protect personal data;

h. The identity of the data processors, both internal or external;

The Data Processors Record of Processing Activities includes all categories of processing activities carried out on behalf of the Data Controller, containing:

a. the name and contact details of the processor or processors and each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

b. the categories of processing carried out on behalf of each controller;

c. transfers of personal data to a third country, including the identification of such country or international organisation and, in the case of transfers referred to in clause 3.11, the documentation of suitable safeguards;

d. a general description of the appropriate technical and organisational security measures that are being implemented.

The Record of Processing Activities shall be reviewed at least annually and, in any case, whenever a significant change is made in any of the processing activities.

No processing activities shall be carried out which could compromise the rights and freedoms of data subjects. To this end, and in compliance with GDPR, an objective risk analysis of each processing will be carried out, as described in the next section.

3.13. OBJECTIVE PRIVACY RISK ASSESMENT AND DATA PROTECTION IMPACT ASSESMENT (DPIA)

The processing activities included in the scope of these BCRs shall go through an objective privacy risk assessment. If the processing results in a high risk to the rights and freedoms of the data subjects, a Data Protection Impact Assessment ("DPIA") shall be carried out. If the DPIA shows that the processing carries a high risk and the controller does not take measures to mitigate it, the supervisory Authority will be consulted before proceeding with the processing.

The DPIA is a more exhaustive analysis of the risks associated with a processing activity that allows for the identification of risk mitigation measures, through:

a. Evaluation of legal and technological threats and vulnerabilities, including their likelihood and potential impact;

b. Calculation of inherent risk;

c. Assessment of the degree of maturity of the safeguards;

d. Calculation of residual risk;

e. Implementation of the Action Plan.

3.14. DATA PROTECTION BY DESING AND BY DEFAULT

The Data Controller applies, both at the time of determining the means of processing and during the processing activity itself, appropriate technical and organisational measures in order to comply with the requirements of the GDPR and BCRs and protect the rights and freedoms of data subjects.

The Controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed.

Before starting any new processing or modifying an existing one, legal and technical requirements shall be analysed to ensure that the processing by the Iberdrola Group is possible in compliance with GDPR, following the internal procedure of the Iberdrola Group *Procedure to guarantee data protection by design and by default.*

4. DATA SUBJECTS RIGHTS

Regarding the processing of personal data, the Group Companies guarantee to the data subjects the following non-renounceable rights:

a. Right of Access, which involves providing information about the personal data available about the data subject.

b. Right to Rectification, by which the data subject shall have the right to obtain the rectification of any personal data that might be inaccurate or incomplete.

c. Right to Erasure or "right to be forgotten", by which the data subject shall have the right to have his or her personal data erased when the circumstances provided in the GDPR occur.

d. Right to Restriction of Processing, by which the data subject shall have the right to request the restriction of the processing of his or her personal data when the circumstances provided in the GDPR occur.

e. Right to Data Portability, by which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured format, and to transmit such data to another Controller.

f. Right to Object, by which the data subject shall have the right to object to his or her personal data being processed for a specific purpose.

g. The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her.

The Group Companies will only make decisions based exclusively on automated processing, including profiling, that produces legal effects on or significantly affects the data subject, if any of the following conditions apply:

- It is necessary for the execution of a contract between the data subject and a Group Company acting as a Data controller.
- It is authorised by the legislation applicable to the Data Controller and appropriate measures are also established to safeguard the rights and freedoms and the legitimate interests of the data subject.
- It is based on the explicit consent of the data subject.

In the first and third cases, the data subject will be given, at least, the right to obtain human intervention by the Data Controller, to express his/her point of view and to challenge the decision.

The exercise of the foregoing rights must be carried out in accordance with the provisions in the applicable data protection regulations, and in any case, in compliance with the provisions of GDPR.

5. RIGHTS OF THIRD PARTIES BENEFICIARIES

The Group Companies shall guarantee data subjects the exercise of the rights to apply these BCRs as third-party beneficiaries. Data subjects may invoke the rights set out it paragraphs 3,4, 7, 10, 11 and 12 of these BCRs, which they are entitled to as third-party beneficiaries in relation to the processing of their data, under the terms provided in this paragraph. Also, the data subjects have the right to easy access these BCRs.

Data subjects whose personal data are collected and/or processed in the EEA by a Group Company (Exporter) and transferred to a Group Company outside the EEA (Importer) shall be entitled to demand compliance with these BCRs as third parties' beneficiaries.

For these purposes:

- **They may file a complaint with the competent supervisory authority** (at their choice, the EEA supervisory authority corresponding to their country of residence, the place of work or the country of alleged infringement) **and with the competent EEA court** (at their choice, those of the EEA country in which the Group Company has an establishment, or those of the country in which the data subject has his/her residence).

- In the event that the Group Company alleged to have breached the BCRs is established outside the EEA, the data subject may, under the terms set out in the preceding paragraph, **exercise his/her rights and file his/her claims**, in accordance with the liability scheme defined in paragraph 12 of these BCRs, against the Group Company which assumes liability in the event of breach of the BCRs by the Group Company domiciled outside the EEA which shall be held liable for the breach. For these purposes, the breach shall be deemed to have occurred at the domicile of the Group Company assuming liability.
- Likewise, the Group Company which, in accordance with the liability scheme defined in paragraph 12 of these BCRs, assumes liability in the event of non-compliance with the BCRs by the Group Company domiciled outside the EEA, shall assume civil liability for **damages suffered by any interested party as a result of non-compliance** with these BCRs by the Group Company or another data importer, provided that such liability has been declared by a court of law or other competent authority.

In order to identify the entity to which the data subject should address their complaint and which is responsible for a BCR breach, the data subject should contact the Global Corporate Security Data Protection Coordinator whose contact details are: dpo@iberdrola.com, who will provide them with the information on the Liable Company.

For the above purposes, these BCRs shall be constantly available and easily accessible by data subjects through publication on the website www.iberdrola.com

6. TRAINING

The Group Companies will promote, update and provide to all employees specific training programs on the principles of personal data protection and specifically on these BCRs and the consequences of non-compliance.

All Group employees must complete the training activities annually and pass an assessment test.

Specific training should be provided to employees who have permanent or regular access to personal data or who are involved in obtaining data or in developing tools to process data.

Annex II to the BCRs includes the training requirements for Group employees in personal data protection and especially in the BCRs as a transfer mechanism between Group companies.

7. CLAIMS MANAGEMENT

Data subjects may at any time contact the Global Corporate Security Data Protection Coordinator, who is competent to deal with and process complaints about a Group Company's failure to comply with the BCRs and who is independent in the exercise of his or her functions. Group Companies must comply with the *Claims Handling Procedure* included as Annex III of the BCRs.

Once a complaint has been filed, it will be acknowledged. The complaint will be resolved within one month of receipt. This period may be extended at maximum by two further months in view of the complexity and number of requests received.

In the event that a complaint gives rise to an investigation by the competent supervisory authority, the Group Company concerned shall respect the decision taken.

8. AUDIT AND SUPERVISION PROGRAM

The Group Companies privacy audit program expressly includes verification of compliance with these BCRs, being established the verification mechanisms in Iberdrola Group's internal procedure known as the *GDPR Compliance Assessment Model*. The *BCRs Audit Procedure* is included as Annex IV.

The Global Corporate Security Data Protection Coordinator determines the scope of the BCRs audit which covers all aspects of the BCRs including methods to ensure that corrective actions are carried out.

The audit of the BCRs may be carried out by internal means or through an external audit. The audit report must be shared with the Boards of Directors of the Group Companies that assume liability in the event of non-compliance with the BCRs and their Local Corporate Security Data Protection Coordinator, and with the Global Corporate Security Data Protection Coordinator, specifying corrective measures, recommendations and a deadline for their implementation.

The audit of the BCRs is annual. The Boards of Directors of the Group Companies that assume liability in the event of non-compliance with the BCRs may also request an audit of the BCRs.

Iberdrola will provide, through the Global Corporate Security Data Protection Coordinator, access to the results of the BCRs audit to the competent European Data Protection Authority upon request by the latter. The competent European Data Protection Authorities may carry out a data protection audit of any member of the BCRs if they deem it appropriate.

Group Companies must adjust their behaviour to the recommendations that the Data Protection Authorities may make regarding the scope and compliance with these BCRs.

9. COMPLIANCE

The Global Corporate Security Data Protection Coordinator is responsible for supervising and ensuring that Group Companies comply with the BCRs in a coordinated manner and following common interpretative criteria, with the assistance of those professionals that integrate the Iberdrola Group's data protection team.

Annex V provides information on the operating structure, coordination mechanisms and responsibilities of the Iberdrola Group's data Protection team, which guarantees compliance with personal data protection throughout the Group.

10. MUTUAL SUPPORT AND COOPERATION WITH DATA PROTECTION AUTHORITIES

The Group Companies undertake to cooperate and assist each other in the event of complaints from a data subject or investigations and consultations by the Supervisory Authorities in relation to BCRs breaches.

The Group Companies further undertake to cooperate with the competent Data Protection Authorities within the scope of application of the BCRs, and will respond to the requests made by said Authorities in relation to the BCRs, in an appropriate form and within the time limit, and shall comply with the decisions and recommendations made by them. To this end, they shall follow the *Procedure for cooperation with the Supervisory Authorities* detailed in Annex VI.

The Group Companies accept being subject to any data protection audits carried out by the Data Protection Authorities.

11. RELATIONSHIP BETWEEN BCRs AND LOCAL LEGAL REGULATIONS

Group Companies must comply with applicable local data protection regulations, without prejudice to respecting these BCRs, as long as BCRs provide for a higher level of protection than that laid down in the local regulations. In all those aspects contemplated in these BCRs in which the applicable local regulations establish a higher level of protection, the local regulations shall apply.

In the event of a conflict between the applicable local regulations and these BCRs in such a way that the BCRs cannot be adequately complied with or has a substantial effect on the guarantees provided by the BCRs, the Group Company concerned must inform the Global Corporate Security Data Protection Coordinator as soon as it becomes aware of the conflict.

Once the Global Corporate Security Data Protection Coordinator has received the appropriate communication, he or she will record the conflict and inform promptly the Liable Companies and all Group Companies that have previously transferred data to the Group Company raising the conflict.

The Local Corporate Security Data Protection Coordinator will bring the conflict to the attention of the competent EEA Supervisory Authority and, together with the Group Company involved, will promote the solution which is most compatible with the principles of GDPR.

When the conflict takes place with the applicable regulations of a third country, the competent EEA Supervisory Authority will be informed. If the company has been required to disclose data, the communication to be made shall include information of the data requested, the requesting body and the legal basis for the disclosure.

In the event that the notification to the competent EEA Supervisory Authority is prohibited, the requested Group Company will make every effort to overcome such prohibition and shall demonstrate that it did so. If, nevertheless, the requested Group Company is unable to notify the competent EEA Supervisory Authority, the requested Group Company undertakes to provide general information on the requests it has received on an annual basis.

Transfers of personal data from a Group Company to any public authority may not be massive, disproportionate or indiscriminate.

12. LIABILITY

With regard to liability, the Iberdrola Group points out the following Group Companies as liable companies ("**Liable Companies**") that accept responsibility for any violation of the BCRs by any of the Group Companies established outside the EEA:

- Iberdrola España, S.A. (Sole-Shareholder Company) will assume liability for any violation of the BCRs when the entity exporting the data is any company located in Spain and dependent on it. Also, Iberdrola España, S.A. (Sole-Shareholder Company) shall assume liability for any violation of the BCRs when the entity exporting the data is Iberdrola S.A., and any company, directly or indirectly owned by Iberdrola, S.A. not dependent on any of the companies indicated in the following paragraphs as Liable Companies.
- Iberdrola Participaciones, S.A. (Sole-Shareholder Company), which will assume liability for any violation of the BCRs when the entity exporting the data is a dependent company located in any country of the EEA.
- Iberdrola Energía Internacional, S.A. (Sole-Shareholder Company), which will assume liability for any violation of the BCRs when the entity exporting the data is any company dependent on it located in any country of the EEA.

Liable company	Entity exporting
Iberdrola España, S.A. (1)	Group Company dependent on Iberdrola España, S.A. and located in Spain (*)
	Iberdrola, S.A.
	Any Group Company, directly or indirectly owned by Iberdrola, S.A. not dependent on any of the companies (2) or (3) (*)
Iberdrola Participaciones, S.A. (2)	Group Company dependent on Iberdrola Participaciones, S.A. and located in any country of the EEA (*)
Iberdrola Energía Internacional, S.A. (3)	Group Company dependent on Iberdrola Energía Internacional, S.L. and located in any country of the EEA (*)

(*) Annex I contains the Group Companies which are bonded to the BCRs, grouped by the Group Companies that directly or indirectly have control over the first ones.

In any case, claims for non-compliance with BCRs by a Group Company may be filed by the data subject by writing to the Global Corporate Security Data Protection Coordinator whose contact details are: dpo@iberdrola.com, or Iberdrola – Calle Tomás Redondo 1 Madrid -28033- Spain as described in Annex III – Claims handling procedure.

The Liable Companies accept:

- That the data subject shall have the rights and remedies against them before the courts or other competent authorities of the EU having jurisdiction according to paragraph 5 of this BCRs, as if the breach had been caused by them in the Member State in which they have their registered office, instead of the Company adhered to the BCRs outside the EEA having breached them.
- That they will pay compensation for any material or immaterial damage resulting from the violation of the BCRs by the Group Companies.
- They shall have the burden of proof to prove that the Company adhered to the BCRs outside the EEA is not liable for any violation of the rules from which a claim for damages has arisen on the part of a data subject.
- Agree to take the necessary measures to remedy the breaches of the BCRs by other Group Companies.

13. UPDATES AND MODIFICATIONS OF THE BCRs

The modification and/or updating of these BCRs will be carried out in accordance with the stipulations of the *Procedure for updating the BCRs* included in Annex VII, which includes the approval process for changes in the BCRs, how the changes shall be communicated to the Data Protection Authorities, to the Group Companies and to those affected. In addition, the Iberdrola Group foresees the annual update of the Iberdrola Group Cybersecurity Framework and the internal procedures referred to in these BCRs.

14. BCRs TERMINATION

In the event of termination of the IA the obligations relating to the rights of third-party beneficiaries, in relation to any personal data within the scope of these BCRs that has been transferred from the EEA prior to the effective date of termination, shall continue.

15. CONTACT

Affected parties may direct any questions about these BCRs, their rights under these BCRs or any other personal data protection issue to the Global Corporate Security Data Protection Coordinator whose contact details are: dpo@iberdrola.com.

If data subjects do not agree with the processing of their personal data by the Group Companies, the *Claims Procedure* set out in Annex III shall be used.

Annexes

ANNEX I – LIST OF COMPANIES INCLUDED IN THE SCOPE OF APPLICATION OF BINDING CORPORATE RULES

The list of Iberdrola of companies included in the scope of application of binding corporate rules is available on the Iberdrola website (www.Iberdrola.com). In it, the first column reflects the corporate name of each Company and, in bold, the companies that directly or indirectly have control over those that appear below each of them. The second column reflects the registered office of each company.

ANNEX II - PERSONAL DATA PROTECTION TRAINING

This document includes information on the training of Iberdrola's Group ("**Group**") employees in personal data protection, and specifically on the BCRs as a mechanism for the transfer of personal data between Group Companies.

The Global Corporate Security Data Protection Coordinator is responsible for defining the training needs in data protection at the Iberdrola Group, and will therefore define the scope and content of the training, to ensure the correct dissemination of the rights, responsibilities and obligations of Iberdrola employees in this area. The Human Resources Learning & Development departments in each country are responsible within the Iberdrola Group for designing and monitoring the Group's staff training plans, which include training in personal data protection. The training actions are approved by the Training Quality Committee of each country, duly recording the approval in the annual Training Plan, approved by the Human Resources Department of each country and communicated, where appropriate, to the trade unions representatives in the company.

Each Learning & Development Department is responsible for ensuring that the training plan is complied with by all employees and informs the respective Human Resources Department of its effective compliance.

All employees of the Iberdrola Group will be included in the training program on personal data protection and the Group's BCRs.

The training will be on-line, keeping in any case a record of the training activity carried out, including the list of employees that have fulfilled the data protection training. For each training there will be carried out test on the knowledge acquired. If the test is not passed, new tests must be carried out until the test is passed.

There will be, therefore, a training record, that includes duration, start and end dates, course content, and name of attendees. Likewise, the latest version of the course will be kept on Iberdrola's Intranet.

In accordance with the above, Iberdrola Group has an annual training plan in personal data protection, designed according to the risks identified in personal data protection in the industry for all employees of Group Companies (within and outside the EEA). Through this training, the necessary measures are adopted to ensure that employees are aware of the requirements deriving from the personal data protection regulations and the BCRs, strictly complying with their obligations relating to the training of employees.

ANNUAL TRAINING PLAN FOR PERSONAL DATA PROTECTION

General training in personal data protection

All employees of the Iberdrola Group companies must undergo an annual general training course on personal data protection. In addition, employees receive training on other procedures and internal rules relating both to the protection of personal data in general and to the BCRs in particular.

New employees receive general training in personal data protection and training and information on the BCRs when they begin their relationship with the Group Company that hired them.

The general training in personal data protection addresses the national and international legal framework on personal data protection, internal policies on personal data protection, protocols, review of practical cases and privacy and security procedures of mandatory compliance in Iberdrola.

The purpose of the general training course on personal data protection is that all employees understand the basic principles of personal data protection, confidentiality and information security and the privacy and information security policies and procedures of Iberdrola.

Binding Corporate Rules Training

All employees of the Group Companies must carry out the training program on Iberdrola BCRs on an annual basis.

The training on BCRs will cover:

1.- Concept

2.- Binding Corporate Rules of the Iberdrola Group

3.- Effectiveness, mandatory compliance and consequences of non-compliance

In view of the roles and responsibilities of employees, specific training will be given on the protocols for updating, claims management and auditing Iberdrola BCRs.

ANNEX III - CLAIMS HANDLING PROCEDURE

The following is the procedure for dealing with claims that a data subject may file to the Iberdrola Group in relation to its personal data processing in accordance with the BCRs.

Making a complaint

Claims for non-compliance with BCRs by a Group Company may be filed by the person concerned by writing to the Global Corporate Security Data Protection Coordinator at: dpo@iberdrola.com or Iberdrola Calle Tomás Redondo 1, Madrid -28033- Spain.

Claim Management

The Global Corporate Security Data Protection Coordinator will be responsible for responding to complaints of non-compliance with the BCRs Rules by Group Companies.

Once a complaint has been filed, the Global Corporate Security Data Protection Coordinator will acknowledge receipt of the complaint and assess compliance with the formal requirements for admission. He or She will then contact the related Local Corporate Security Data Protection Coordinators, who will be responsible for providing the information necessary to resolve the claim.

The Global Corporate Security Data Protection Coordinator will coordinate the response to the data subject. The complaint will be resolved within one month of receipt. This period may be extended to a maximum of two months in view of the complexity and number of requests received. However, the claimant will be informed and an explanation will be provided. The data subject shall be informed of the consequences if the claim is rejected or if the claim is justified.

Data subjects may at any time contact the Global Corporate Security Data Protection Coordinator, who is responsible for dealing with BCRs related claims by a Group Company, and who is independent in the exercise of his or her functions.

Other means of complaint

The data subject will have the right to demand compliance with these BCRs by means of a claim before a Supervisory Authority or the exercise of actions before the Courts. For these purposes:

- Data subjects may file a complaint with the competent supervisory authority (at their choice, the EEA supervisory authority corresponding to their country of residence, place of work or the country of the alleged infringement) and with the competent jurisdictional body of the EEA (at their choice, the country of the EEA in which the Group Company has an establishment, or the country in which the data subject resides).

  In the event that a claim gives rise to an investigation by the competent supervisory authority, the Group Company concerned shall respect the decision taken.

- In the event that the Group Company that has allegedly breached the BCRs is established outside the EEA, the data subjects may, under the terms set out in the previous section, exercise their rights and file a claim in accordance with the scheme of liability defined in the BCRs against the Group Company that assumes responsibility in the event of a breach of the BCRs by any of the Group Companies located outside the EEA, which will be held responsible for the breach. For these purposes, the breach shall be understood to have occurred in the residence of the Group Company, which takes the responsibility.

- Likewise, the Group Company which, in accordance with the liability scheme defined in the BCRs, assumes responsibility in the event of non-compliance with the BCRs by any of the Group Companies established outside the EEA, shall assume civil liability for the damages suffered by any data subject for non-compliance with these BCRs by any Group Company or other data importing company, provided that such liability has been declared by a court or other competent authority.

With regard to liability, the Iberdrola Group points out the following Group Companies as liable companies (“**Liable Companies**”) that accept responsibility for any violation of the BCRs by any of the Group Companies established outside the EEA:

- Iberdrola España, S.A. (Sole-Shareholder Company), which will assume liability for any violation of the BCRs when the entity exporting the data is any company located in Spain and dependent on it. Also, Iberdrola España, S.A. (Sole-Shareholder Company) shall assume liability for any violation of the BCRs when the

entity exporting the data is Iberdrola S.A., and any company, directly or indirectly owned by Iberdrola, S.A. not dependent on any of the companies indicated in the following paragraphs as Liable Companies.

- Iberdrola Participaciones, S.A. (Sole-Shareholder Company), which will assume liability for any violation of the BCRs when the entity exporting the data is a dependent company located in any country of the EEA.
- Iberdrola Energía Internacional, S.L. (Sole-Shareholder Company), which will assume liability for any violation of the BCRs when the entity exporting the data is any company dependent on it located in any country of the EEA.

The Liable Companies accept:

- That the data subject shall have the rights and remedies against them before the courts or other competent authorities of the EU having jurisdiction according to paragraph 5 of the BCRs, as if the breach had been caused by them in the Member State in which they have their registered office, instead of the Company adhered to the BCRs outside the EEA having breached them.
- That they will pay compensation for any material or immaterial damage resulting from the violation of the BCRs by the Group Companies.
- They shall have the burden of proof to prove that the Company adhered to the BCRs outside the EEA is not liable for any violation of the rules from which a claim for damages has arisen on the part of a data subject.
- Agree to take the necessary measures to remedy the breaches of the BCRs by other Group Companies.

ANNEX IV – BCRs AUDIT PROCEDURE

The internal document of the Iberdrola Group in which the verification mechanisms are clearly established is the Compliance Assessment Model - European Data Protection Regulation. This verification programme is based on the Iberdrola Group's compliance model, which is applicable to all the Group Companies included in the BCRs scope of application and is founded upon five pillars:

- Governance Framework;
- Methodologies and tools: Record of Processing Activities, Risk Analysis and Data Protection Privacy Impact Assessment (DPIA);
- Procedures, Rules and Guidelines;
- Security measures;
- Compliance assessment and reporting.

In this verification programme participate the personal data protection responsible of the different businesses and corporate areas, as well as the global and local Data Protection Coordinators that make up the Iberdrola Group's Privacy Team. External and internal auditors will also participate.

Assessment of compliance

The compliance assessment system is structured around the pillars of the Iberdrola Group's data protection compliance model.

One of the main elements of the Governance Framework are the BCRs, as a mechanism for transferring personal data between Group Companies.

In their evaluation it will be reviewed:

- The legal instruments enabled to make the BCRs binding internally.
- The guarantees offered by Group companies in relation to the rights of third-party beneficiaries.
- Actions for cooperation and assistance between Group companies in the event of complaints by a data subject or investigations and consultations by the Supervisory Authorities in relation to breaches of the BCRs.
- Cooperation actions with competent Data Protection Authorities and response to requests made by these Authorities in relation to the BCRs in the corresponding form and term and compliance with the decisions and recommendations made by them.
- The management of claims regarding non-compliance with the BCRs by one of the Group Companies.
- The protocol for updating and modifying the BCRs.
- The way in which information on the BCRs is provided to data subjects.
- Compliance with the training plan on BCRs.
- Decisions taken in relation to the mandatory requirements of national legislation that conflict with the BCRs.
- The text of the BCRs will be reviewed to ensure alignment with the Data Protection Governance Framework.

Data Protection Reporting

On a quarterly basis, a reporting of data protection indicators on a local and global level is prepared, which includes certain information, by corporate area/business and country, in relation to BCRs, for example:

- Number of complaints received regarding non-compliance with the BCRs.
- Number of companies adhered to the BCRs.
- Number of requests received from the competent supervisory authorities with respect to the Binding Corporate Regulations.

It will be reported to the Global Corporate Security Data Protection Coordinator and the Boards of Directors of the Group Companies that assume liability in the event of non-compliance with the BCRs and their Local Corporate Security Data Protection Coordinator, along with the identification of potential data protection risks, which will be included in the Key Risk Report.

ANNEX V- IBERDROLA'S PRIVACY TEAM

The following is a description of the Iberdrola Group's privacy team, which is integrated by data protection professionals whose purpose is to globally comply with the protection of personal data within the Group and in particular with the BCRs.

Global operational structure

A **Global Corporate Security Data Protection Coordinator ("Global Coordinator")** has been appointed, within the Corporate Security Department of the Iberdrola Group. The responsibilities of the Global Coordinator are the following:

- Propose and promote the update of the Global Data Protection Framework (hereinafter, Global DP Framework) and the Global Data Protection rules.
- Define the global data protection management system, including, among others, global rules and procedures and corporate methodologies & tools, and promote and supervise its implementation across the Group.
- Define global security standards applicable to Personal Data Protection for both internal processing and third parties.
- Provide advice, recommendations and clarifications over the content of the rules, methodologies and tools, global standards and the Global DP Framework.
- Establish a global compliance assessment and coordination system, in order to assess noncompliance risks and effectiveness of the *Data Protection Policy* and the Global DP Framework and report to the Global Cybersecurity Committee and the Compliance Office.
- Act as main interlocutor with the Data protection supervisory authority for any issue that impact the Group as a whole, with the support of Legal Services.
- Coordinate the functions and tasks of the Local Data Protection Coordinators in Corporate Security, in order to promote the implementation of data protection best practices and the global strategy of the Group.
- Comply with the Data Protection Officer functions according with the GDPR and report to the Board of Directors of Iberdrola, S.A.
- Monitor and ensure compliance with the BCRs in a coordinated and homogenous manner, with the support of the Global and Local Data Protection Coordinators of the Iberdrola Group.

The Corporate Security Department will be supported by a **Global Data Protection Coordinator in Legal Services**, who will provide support in the definition of the global governance framework, the rules and contracts related to intragroup Personal Data transfer, as well as in the development of the rest of his or her functions.

Additionally, most relevant business and corporate areas have designated a **Global Data Protection Coordinator**, in order to ensure alignment of data protection management systems, in their area of responsibility, with corporate standards and compliance with applicable laws and regulations, as for example, and to the extend applicable, the existence of a Record of Processing Activities, privacy risks analysis , an incident reporting system, etc..; communicate and act as key interlocutor and support with the specific business or corporate area at a subholding and head of business level, promoting global strategy implementation and the sharing of best practices in all the Group Companies.

All aforementioned coordinators will be part of the **Global Cybersecurity Committee**, established in compliance with the *Cybersecurity Risk Policy* whose function is to supervise the general state of Cybersecurity and Personal Data protection in the Group, facilitates coordination and supports the Corporate Security Department in the implementation of approved measures, all in accordance with the terms set forth in its internal Regulations.

Operating structure in each subholding

In each subholding, a **Local Corporate Security Data Protection Coordinator** has been designated by the Corporate Security Departments, who shall ensure local implementation of the global data protection strategy, taking into account each country specificities.

Those Local Corporate Security Data Protection Coordinator of the Group Companies is responsible for data protection at a local level, comply with the Data Protection Officer functions according with the GDPR, and report the Board of Directors of the relevant subholding.

In that sense, the Local Corporate Security Data Protection Coordinator will ensure that there is an adequate level of coordination with the Global Data Protection Coordinator, with regards to key data protection relevant matters, as key initiatives, risk indicators and data protection incidents.

Likewise, the Corporate Security departments in each subholding companies will promote the local implementation of global data protection strategy, and compliance with applicable laws and regulations, while also ensuring coordination with the different business and corporate areas.

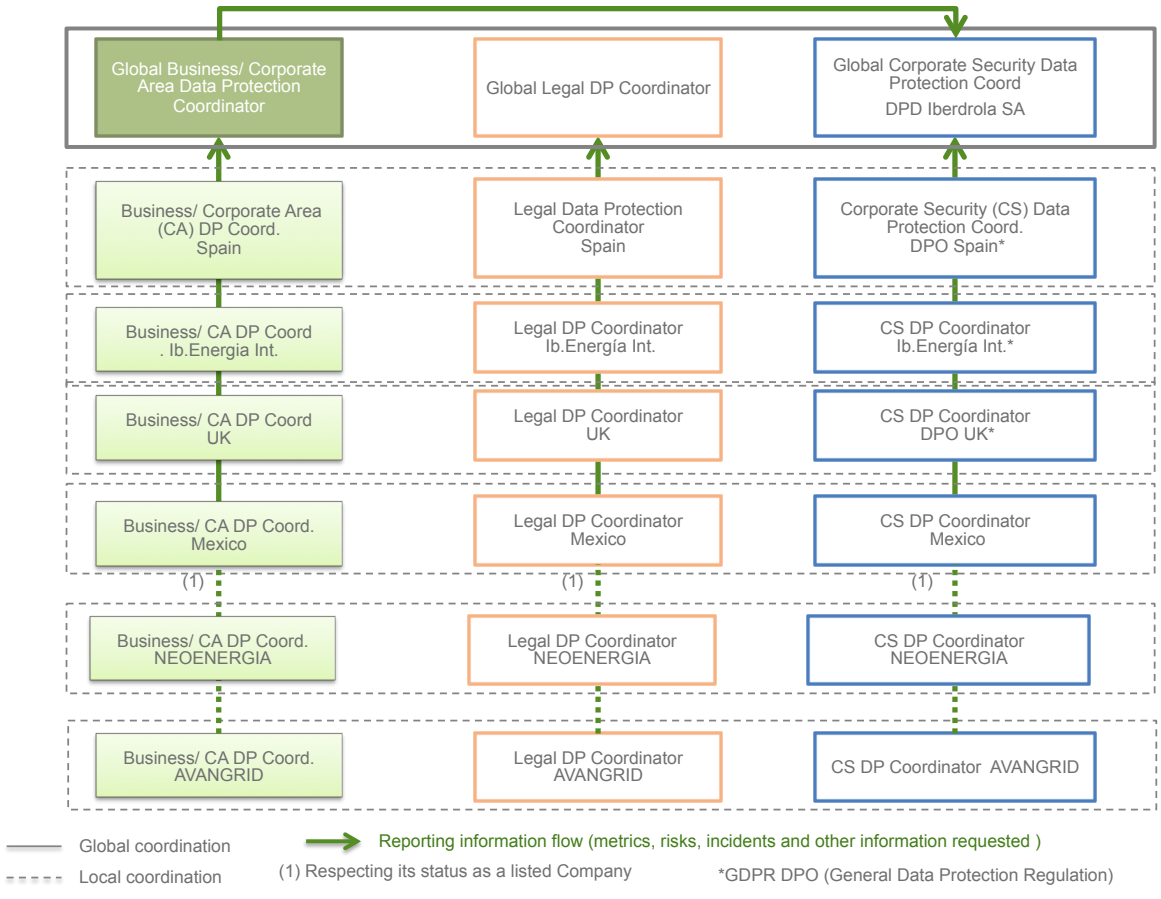
Those Corporate Security departments have set up local data protection coordination groups to support the Local Corporate Security Data Protection Coordinator in the fulfilment of his/her responsibilities. To this end, the subholding companies have also appointed a **Local Data Protection Coordinator in Legal Services** and their respective **Local Data Protection Responsible in the relevant business and corporate areas**, who assume the corresponding responsibilities and coordinate with their global counterpart. These local coordination groups meet periodically in order to adopt any required measures to ensure that global rules and guidelines are implemented locally.

Coordination Mechanisms

To ensure adequate coordination among Group Companies, in line with the group corporate structure, the following mechanisms have been established:

- **Local operational coordination** among Local Business/Corporate Area Data Protection Responsibles, Local Data Protection Coordinator in Legal Services and Local Corporate Security Data Protection Coordinator, through the local data protection coordination group.
- **Global operational coordination** among the Global Data Protection Coordinator in Legal Services, Business/Corporate Areas, and Global Corporate Security Data Protection Coordinator, through the Global Cybersecurity Committee.
- **Operational coordination per business/corporate area**: The Local Data Protection Coordinators and Responsibles shall inform the corresponding Global Data Protection Coordinators about data protection key indicators, incidents and relevant risks.

The diagram below depicts this coordination and reporting mechanisms among Business and Corporate Areas Data Protection Responsibles, and global and local data protection coordinators.



Both the Global Coordinator and those Local Corporate Security Data Protection Coordinator report to the highest level of management in the Iberdrola Group.

ANNEX VI - COOPERATION PROCEDURE WITH THE SUPERVISORY AUTHORITIES

The following is the procedure for cooperation with the European Data Protection Supervisory Authorities in relation to Iberdrola BCRs.

Group Companies further undertake to cooperate with the competent Data Protection Authorities within the scope of application of the BCRs, and will respond to the requests made by said Authorities in relation to the BCRs, in an appropriate form and within the time limit, and shall comply with the decisions and recommendations made by them.

The Global Corporate Security Data Protection Coordinator will provide, upon request, access to the BCRs audit reports, to the competent European Data Protection Supervisory Authorities.

Based on the commitment of cooperation and assistance between Group Companies in the investigations and queries of the Data Protection Supervisory Authorities in relation to BCRs compliance, the response to any request from a Supervisory Authority will be managed by the Local Corporate Security Data Protection Coordinators who will inform the Global Corporate Security Data Protection Coordinator who, with the support of legal services, will respond to it.

ANNEX VII - BINDING CORPORATE RULES UPDATING PROCEDURE

The following is the procedure for updating Iberdrola BCRs, which includes the process for approving changes to the BCRs, and how changes are notified to the Data Protection Authorities, to the Group Companies and to the data subjects.

Modifications to the Binding Corporate Rules

Amendments to the BCRs are those that may affect the level of protection offered by them or significantly affect the BCRs, as for example, changes in legislation or in the structure of the Group.

Amendments to the BCRs must be approved by the Global Corporate Security Data Protection Coordinator and communicated to the Global Cybersecurity and Data Protection Committee for acknowledgment.

Iberdrola, S.A. shall inform the Spanish Data Protection Agency of any proposed amendment to the BCRs within a maximum period of fifteen (15) days, so that such Authority may determine whether the proposed amendment shall be submitted to the cooperation procedure for approval of BCRs. The modification shall not be carried out until it has been approved by the Spanish Data Protection Agency.

Binding Corporate Rules Updates

BCRs updates are, for example, changes to the list of Group Companies subject to them.

Updates to the BCRs will be approved by the Global Corporate Security Data Protection Coordinator and communicated to the Global Cybersecurity Committee for acknowledgment and implementation.

The **Global Corporate Security Data Protection Coordinator** will communicate any update of the BCRs to the Spanish Data Protection Agency at least once a year, with a brief explanation of the reasons justifying the update, and will provide the necessary information to those affected or to the Data Protection Authorities that request it.

Binding Corporate Rules Record of modifications and communication of changes

BCRs are subject to a record of modifications, which includes the date on which they are reviewed and the changes made as a result of such review. The **Global Corporate Security Data Protection Coordinator** will maintain an updated record of the amendments to the BCRs and an updated list of the Group Companies subject to the BCRs and will be responsible for communicating the amendments and updates to the Spanish Data Protection Agency.

The **Global Corporate Security Data Protection Coordinator** will also be responsible for communicating promptly or without undue delay any changes to the BCRs by direct notification to the Spanish Data Protection Agency, as well as to any other competent Supervisory Authority and to the Group Companies.

Information regarding the BCRs changes to the data subjects shall be made through publication on the IBERDROLA intranet and the corporate website, including other means such as general communications.

The **Global Corporate Security Data Protection Coordinator** will ensure that all new Group Companies adhere to the BCRs by signing the corresponding adherence agreement and effectively implement them, before personal data is transferred them.


IBERDROLA