

# Iberdrola's Group Binding corporate rules

September 2025



Iberdrola

# Content

---

<b>INTRODUCTION</b>	<b>2</b>
<b>1. DEFINITIONS</b>	<b>2</b>
<b>2. SCOPE OF APPLICATION</b>	<b>4</b>
2.1. Material scope of application of the BCRs	4
2.2. Geographical scope of application of the BCRs	5
<b>3. PRINCIPLES</b>	<b>6</b>
3.1. Compliance with local laws and GDPR	6
3.2. Lawfulness, fairness and transparency	6
3.3. Purpose limitation	8
3.4. Data minimization	8
3.5. Accuracy	8
3.6. Storage limitation	8
3.7. Processing of special categories of personal data	9
3.8. Integrity and confidentiality	9
3.9. Personal data security breaches	10
3.10. Processing carried out by data processors	10
3.11. International processing of personal data	11
3.12. Record of processing activities	12
3.13. Objective privacy risk assessment and data protection impact assessment (DPIA)	13
3.14. Data protection by design and by default	14
<b>4. DATA SUBJECTS RIGHTS</b>	<b>14</b>
<b>5. THIRD PARTY BENEFICIARIES' RIGHTS</b>	<b>15</b>
<b>6. Training programme</b>	<b>15</b>
<b>7. Internal complaints handling procedure</b>	<b>16</b>
<b>8. Audit and supervision programme</b>	<b>16</b>
<b>9. COMPLIANCE</b>	<b>17</b>
<b>10. MUTUAL ASSISTANCE AND COOPERATION DUTY WITH DATA PROTECTION AUTHORITIES</b>	<b>17</b>
<b>11. RELATIONSHIP BETWEEN BCRs AND LOCAL LEGAL REGULATIONS</b>	<b>18</b>
<b>12. LIABILITY</b>	<b>19</b>
<b>13. UPDATE AND MODIFICATIONS OF THE BCRs</b>	<b>21</b>
<b>14. TERMINATION OF THE BCRs</b>	<b>21</b>
<b>15. CONTACT</b>	<b>21</b>

<b>ANNEX I – List of the companies included in the scope of the binding corporate rules</b>	<b>23</b>
<b>ANNEX II - Training in personal data protection</b>	<b>23</b>
Annual training programme in personal data protection	23
<b>ANNEX III – Complaints handling procedure</b>	<b>24</b>
<b>ANNEX IV – BCRs audit procedure</b>	<b>26</b>
<b>ANNEX V- Iberdrola's group privacy team</b>	<b>27</b>
<b>ANNEX VI - Procedure for cooperation with supervisory authorities and other public authorities</b>	<b>30</b>
<b>ANNEX VII – Procedure for updating iberdrola's binding corporate rules</b>	<b>31</b>

**NOTICE:**

This document is a translation of a duly approved Spanish-language document, and is provided for informational purposes only. In the event of any discrepancy between the text of this translation and the text of the original Spanish-language document that this translation is intended to reflect, the text of the original Spanish-language document shall prevail.

---

## INTRODUCTION

---

The Binding Corporate Rules (hereinafter “**BCRs**”) demonstrate the global commitment of all the companies that comprise the Iberdrola Group and are bound by these BCRs (Iberdrola, S.A., the company that exercises control, and all its controlled companies that are also bound by these BCRs, hereinafter referred to as the “**Iberdrola Group**” and each of its affiliated companies, the “**Group Companies**”) to privacy and data protection, and establish the framework of appropriate safeguards for the transfer and processing of personal data among them.

These BCRs are adopted in accordance with the provisions of Regulation (EU) 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/EC (hereinafter, the “**GDPR**”).

These BCRs apply to all personal data processed within the European Economic Area (hereinafter, the “**E.E.A.**”), by Group Companies acting as data controllers or processors on behalf of a Group data controller, and transferred, directly or indirectly, from Group Companies located in the E.E.A to Group Companies located outside the E.E.A, to the processing of personal data falling within the scope of these BCRs.

The obligations set out in these BCRs apply to all Group Companies acting as Controllers, as well as to Group Companies acting as internal Data processors.

By adhering to these BCRs, the Group Companies commit to respecting and complying with their provisions relating to the collection and processing of personal data for the fulfilment of their own purposes, and to ensure compliance by all their employees.

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

These BCRs and the Group Companies are published on the website [www.iberdrola.com](http://www.iberdrola.com), and on Iberdrola's Group Intranet.

---

## 1. DEFINITIONS

---

- a. “**Personal Data**” means any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- b. “**Special categories of personal data**”: Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's life or sexual orientation.
- c. “**Processing**” means any operation or set of operations which is performed on personal data or 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, suppression or destruction.
- d. “**Data controller**” means the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In these BCRs, the Data controller will be the Group Company transferring the personal data and the Group Company receiving the data when it is processed by the Company for its own purposes.

- e. **“Data processor”** means a natural or legal person, public authority, service or other body that processes personal data on behalf of the controller.

For the purposes of these BCRs, the Group Company providing the services will be considered as a processor in accordance with the corresponding service agreement.

- f. **“Recipient”** means a natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not.
- g. **“Third party”**: means a natural or legal person, public authority, service or other body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process the personal data.
- h. **“Iberdrola Group or Group”**: a group consisting of Iberdrola, S. A., the company exercising control, and all its controlled companies.
- i. **“Group Company/Companies”**: each of the companies within Iberdrola's Group that have adhered to the BCRs by signing the Intragroup Agreement on the BCRs.
- j. **“Parent Company”**: in accordance with the Spanish Commercial Code, within Iberdrola's Group the parent company is the Group Company that meets any of the requirements in relation to the other subsidiary companies:
1. Holds the majority of the voting rights.
  2. Has the authority to appoint or remove the majority of the members of the administrative body.
  3. Can exercise, by virtue of agreements made with third parties, the majority of the voting rights.
  4. Has appointed with its votes the majority of the members of the administrative body who are in office at the time the consolidated accounts are to be drawn up and during the two immediately preceding financial years.
- k. **“Subholding company”**: a company that groups together in Spain, the United Kingdom, the United States, Mexico and Brazil the companies of Iberdrola's Group that are domiciled in such countries and that do not directly depend on Iberdrola, S.A. Exceptionally, Iberdrola Energía Internacional, S.A. groups together the Companies of the Iberdrola Group that do not depend on any of the abovementioned subholding companies and that do not directly depend on Iberdrola, S.A. The subholding company directly depends on Iberdrola, S.A. and, therefore, its subsidiaries are part of the Iberdrola Group.
- l. **“Binding Corporate Rules”**: personal data protection policies adhered to by a Group Member established in the territory of a Member State for the transfer or for the set of transfers of personal data to a Data controller or a Data processor based in one or more third countries, within a business group or a union of companies engaged in a joint economic activity.
- m. **“Supervisory Authority”** means the independent public authority established by a Member State to monitor and coordinate the implementation of the GDPR.
- n. **“Public Authority”** means the public authority established in the Importing country which, in compliance with the laws of that country, requests access to the Exporter's Personal Data of the Data transferred under the BCRs.



- o. **“Spanish Data Protection Agency”**: refers to the Supervisory Authority responsible for overseeing and coordinating the procedure for authorising BCRs, approving them, and informing the relevant Supervisory Authorities of any updates to the BCRs or the list of BCR members.
- p. **“Data Subject”**: the identified or identifiable natural person to whom the personal data being transferred from the E.E.A to third countries belongs.
- q. **“Data Exporter”** means a Group Company established in an E.E.A country, which directly or indirectly transfers personal data to another Group Company not established in an E.E.A country.
- r. **“Data Importer”** means a Group Company which, not being in a country of the E.E.A., receives personal data from a data exporter.
- s. **“Security measures”** means appropriate technical and organisational measures taken to ensure a level of security appropriate to the risk.
- t. **“Consent”** means any freely given, specific, informed and unambiguous statement by which the Data Subject agrees, either by a statement or a clear affirmative action, to the processing of personal data concerning him/her.
- u. **“Third country”** means a country that is established outside the E.E.A.
- v. **“Member State law”** refers to the national law of an EU member state, and the law of the E.E.A countries.

To the extent not provided for in this paragraph, the Group Companies shall interpret these BCRs in accordance with the GDPR.

---

## 2. SCOPE OF APPLICATION

---

### 2.1. Material scope of application of the BCRs

The BCRs cover the following processing of personal data:

- **Candidates for a job within the Iberdrola Group**: Identification and curriculum data of candidates applying for jobs and study internships who register on Iberdrola's Group employment portal, in order to allow their participation in possible employment selection processes or student internships. Your personal data may be transferred to any Group Company, even outside the E.E.A, which has an interest in your profile.
- **Employees**: Personal data of employees that are obtained as a result of the employment relationship, in the process of formalizing the relationship and during the period in which it is maintained. Such data may be communicated to the Group Companies, including those outside the E.E.A, for the internal filling of vacancies, for managing the employment relationship, including the management of powers of attorney, guaranteeing compliance with the Code of Ethics, service contracts, and for the team management and organisation. All these international transfers are necessary for the management and fulfilment of the employment relationship with the employee.
- **Participants in scholarship programs**: Identification, academic and professional data of applicants and beneficiaries of scholarship programs, for the purposes of managing and awarding scholarships. The data provided by the applicant will be included in a database accessible to the Group companies involved in the program's management, including those located outside the E.E.A.
- **Volunteers**: Identification data of volunteers, for the purpose of managing Iberdrola's corporate volunteering program and related activities. These data may be communicated to the Iberdrola Group companies coordinating volunteer actions, including those located outside the E.E.A.

- **Suppliers:** Personal identification data, personal and professional characteristics, commercial information, economic and transactional data of suppliers, for the purpose of comprehensive supplier management. These data may be communicated to the Group companies involved in supplier management, including those located outside the E.E.A.
- **Legal representatives:** Identification data and personal and professional characteristics for the purpose of managing powers of attorney. These data may be transferred to Group companies, including those located outside the E.E.A, for the management of representation procedures, powers of attorney, and other appointments within the Iberdrola Group companies.
- **Event attendees and site visitors:** Identification data, including images, of attendees at events and visitors to Iberdrola Group facilities, for the purpose of managing corporate events and visits and ensuring their security. These data may be communicated to other Iberdrola Group companies, including those located outside the E.E.A, for internal administrative purposes.
- **Individuals affected by security incidents and/or threats:** Identification data of individuals affected by security incidents, as well as any other data related to detected security incidents and/or threats (e.g., IP addresses, usernames, passwords, etc.). These data may be communicated to Group companies, including those located outside the E.E.A, for the purpose of managing such incidents and/or threats.
- **Individuals contacting Iberdrola through mailboxes and other channels:** Identification data of individuals who contact Iberdrola through dedicated mailboxes or other channels to submit queries, requests, complaints, reports, or similar communications regarding various matters (e.g., privacy, ethics and compliance), as well as any other personal data provided through these channels and data relating to third parties involved in the communication. These data may be transferred to Group companies, including those located outside the E.E.A, to manage such communications.
- **Third parties in compliance matters:** Identification data, personal and professional characteristics, commercial and employment-related information of natural and legal persons who interact or may interact with Iberdrola, such as suppliers, their attorneys-in-fact, representatives, directors, managers, and shareholders. The purpose is to ensure coordination, implementation, and standardization of compliance practices within the Group, monitor indicators related to business ethics, and prepare the non-financial reporting statement.

## 2.2. Geographical scope of application of the BCRs

These BCRs apply to the transfers of personal data specified referred to in section 2.1 above, regulating the material scope of these BCRs, carried out by Group Companies in their capacity as Data controllers or processors. Therefore, these BCRs apply to the Group Company located in an E.E.A. country that exports personal data, directly or indirectly, and to the Group Company located outside an E.E.A. country that imports the personal data.

The BCRs apply to the initial transfers of personal data as well as to onward transfers.

These BCRs are binding on the Group Companies that have signed the Intragroup Agreement on the BCRs (hereinafter, the “IA”) in which they express their acceptance, and which is included as an annex to such IA. Likewise, Annex I of these BCRs includes a list of the Group Companies bound by these BCRs, grouped by the Group Companies that directly or indirectly have control over the former. If you have any questions relating to the Group Companies bound by these BCRs, please contact the Global Corporate Security Data Protection Coordinator whose contact details are: [dpo@iberdrola.com](mailto:dpo@iberdrola.com).

In accordance with the GDPR and applicable labour legislation, these BCRs are binding and enforceable for Iberdrola's Group employees in all Group Companies. Employees have been informed of their existence, indicating that they are mandatory regulations and establishing that, in accordance with the applicable legislation and the employment contracts with each of the Group Companies,



these companies may apply the corresponding disciplinary regime in the event of non-compliance with them.

The processing activities and categories of personal data covered by the BCRs are those defined in their scope of application and apply to both manual and automated processing. The transfers of personal data take place between Group Companies in the normal course of their activities, and such data may be stored in centralized databases accessible by Group Companies from anywhere in the world where Iberdrola Group operates. Although all personal data falling within the scope of these BCRs could potentially be transferred to any third country where a Group Company is located, actual transfers only take place when necessary for a specific processing activity and in compliance with applicable data protection regulations.

---

## 3. PRINCIPLES

---

Any processing of personal data carried out by the Group Company, whether as Data controllers or Data processors, must comply with the following principles, which are implemented through the rules, procedures, methodologies and corporate tools of Iberdrola's Group.

### 3.1. Compliance with local laws and GDPR

In addition to complying with these BCRs, each of the Group Company must comply with the applicable local laws related to personal data, understood as the regulations of the country where it is established and shall ensure that the collection and use of personal data are carried out in accordance with those laws.

### 3.2. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and transparently in relation to the Data Subject. The processing of data is lawful if it is based on any of the following conditions provided for in the GDPR:

- a. **Consent:** the Data Subject has consented to the processing of his/her personal data for one or more specific purposes. For example, the processing of employee images by the Group Companies for social and corporate communication purposes is carried out if the owner has provided his or her consent.

In the event that consent is the legitimate basis for the processing, the Data controller must ensure that the consent has been obtained in the following manner:

1. **Freely given:** consent is considered freely given if the Data Subject has a real option not to give it.
2. **Specific:** the purposes of the processing must be specific and cannot be vague or expanded once the Data Subject has consented to the collection of data.
3. **Informed:** it is necessary for the Data controller to inform the Data Subject of the purposes of the processing, and when necessary, provide additional information to ensure that the Data Subject fully understands the processing activities.
4. **Unambiguous:** consent must expressly refer to each particular processing activity of personal data.

Consent must be obtained independently from the acceptance of any terms and conditions related to the legal relationship and must use clear and simple language.

A record will be kept of when and how the Data Subject's consent was obtained, as well as for what specific purpose, along with the supporting documentation.

In addition, the Data controller must ensure that the Data Subject can withdraw its consent at any time as easily as it was given.

- b. **Contractual relationship:** the processing is necessary for the performance of a contractual relationship between the Group Company and the Data Subject or for the implementation of pre-contractual measures requested by the Data Subject.
- c. **Legal obligation:** the processing is necessary for compliance with a legal obligation to which the controller is subject to.
- d. **Vital interest:** the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- e. **Public interest:** the processing is necessary to ensure that the Data controller fulfils a task carried out in the public interest.
- f. **Legitimate interest:** the processing is necessary for the purposes of the legitimate interests pursued by the Data controller or by a third party, except where such interests are overridden by the interests or 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 involving their personal data. Specifically, the following information should be provided:

- a. The identity and contact details of the Data controller and, where applicable, of its representative.
- b. The contact details of the Data Protection Officer.
- c. The purposes of the processing.
- d. The legal basis or legitimacy for the processing. In the event that the legal basis is the legitimate interest pursued by the Data controller or a third party, provided that this interest is not overridden by the interests or fundamental rights and freedoms of the Data Subject that require the protection of personal data, information will be provided on said interest.
- e. Categories of personal data processed.
- f. The data retention period or the criteria used to determine such period.
- g. The existence of automated decision-making or profiling.
- h. If there are data transfers to third parties, the recipients or categories of recipients must 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 failure to provide such data.
- j. If the Data controller intends or not to carry out international transfers of data to third countries, and, if carried out, the safeguards that will apply to them.
- k. The rights that correspond to you in terms of data protection. These are: the right of access, right to rectification, erasure, restriction of the processing, the right to receive notification regarding rectification or erasure of personal data or restriction of processing, the right to object to processing, the right to data portability, and the right to not to be subject to decisions based solely on automated processing, including profiling. If the 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 intended to uniquely identify a natural person, data relating to the sexual life or sexual orientation of a natural person, the Data Subject will be informed of the right to withdraw its consent at any time.

- l. The right to lodge a complaint with a Supervisory Authority in the event that the Data Subject considers that its personal data protection rights recognized in the applicable regulations or in these BCRs have not been respected.
- m. The existence of automated decisions, including profiling and meaningful information on the logic applied, as well as the significance and consequences of such processing for the Data Subject.
- n. Where the controller intends to further process the personal data for a purpose other than the purpose other than that for which the personal data were collected, it shall provide the Data Subject prior to that further processing with information on that other purpose and with any relevant further information in accordance with the previous sections.
- o. If the data is not obtained from the Data Subject, in addition to the information indicated in the previous sections, the controller shall provide the Data Subject with information on the source of the personal data and, if applicable, whether it comes from publicly accessible sources.

### 3.3. Purpose limitation

Personal data are collected for specific, explicit and legitimate purposes and will not be processed for purposes incompatible with those for which they were originally collected. For example, the registration of a supplier only requires the information necessary to maintain and manage the business relationship (general identification and contact data, bank and transactional data such as invoices and contracts) and is only processed for that purpose and will not be processed for purposes for which it is not intended to be used.

### 3.4. Data minimization

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 complete details of its suppliers, while access to other Group Companies suppliers' information is restricted to the general details of such suppliers (identification, contact and bank details).

### 3.5. Accuracy

Personal data must be accurate and kept up to date. In particular:

- a. All information repositories, including applications, databases, spreadsheets, etc., should include, as far as possible, a data validation mechanism to ensure that the information is accurate and complete.
- b. Processes of periodic review and continuous improvement of the information will be established to ensure that the data are accurate and up to date.

### 3.6. Storage limitation

Personal data must be kept in a form which permits the identification of the Data Subjects for no longer than is necessary for the purposes of the processing. In particular:

- a. All processings of personal data are linked to retention periods implemented through a manual or automatic process which is in the Record of Processing Activities.

- b. Personal data is not retained for a period longer than that implemented through manual or automatic processes.
- c. Mandatory retention periods for the data, without prejudice to their blocking once the processing for which the data was collected has been completed, are those resulting from the legislation, standards and other applicable regulations, both state and sectoral, in each case.

### 3.7. Processing of special categories of personal data

Group Companies are prohibited from processing special categories of personal data, unless there is a legitimate basis for processing as provided for in Article 6.1 of the GDPR, and one of the circumstances set forth in Article 9.2 of the GDPR applies, which exempts the general prohibition on the processing of special categories of data. These circumstances are:

- a. **The Data Subject has given explicit consent** to the processing of such special categories of personal data for one or more of the specified purposes, and such consent is considered valid in accordance with applicable law and regulations;
- b. **The processing is necessary for the fulfilment of obligations and the exercise of specific rights** of the controller or the Data Subject in the field of labour law, social security and social protection, to the extent permitted by the applicable law that establishes adequate safeguards for respecting fundamental rights and interests of the Data Subject;
- c. **The processing is necessary to protect the vital interests** of the Data Subject or another natural person, in the event that the Data Subject is not physically or legally capable of giving consent;
- d. **The processing relates to personal data** that the Data Subject has manifestly made public;
- e. **The processing is necessary for the establishment, exercise or defence of claims** or when the courts act in the exercise of their judicial function.

### 3.8. Integrity and confidentiality

Personal data is processed in a manner that guarantees its security, applying appropriate technical and organizational measures.

To guarantee this principle, the personal data in relation to which a Group Company is the Data controller or Data processor must be processed:

- a. Safely and with adequate protection against unauthorised or unlawful processing and against accidental or unlawful loss, destruction or alteration. To this end, the security measures considered necessary will be implemented in each case depending on the level of risk of the processing activity in question.
- b. Under conditions that guarantee the permanent confidentiality, integrity, availability and resilience of the systems and processing services.
- c. Under conditions that ensure the ability to quickly restore 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 personal data, and their processing must be subject to processes of verification, evaluation and periodic assessment of effectiveness.

Group Companies must comply with Iberdrola's Group Cybersecurity Framework, which defines the programme, policies, standards and processes necessary to manage cybersecurity risks in Iberdrola's operating environment.



### 3.9. Personal data security breaches

In the event of a security breach that results in the destruction, loss, accidental or unlawful alteration of personal data, as well as any unauthorised communication or access to personal data transmitted, stored or otherwise processed, the Group Company acting as Data controller or Data processor of the processing must proceed in accordance with the provisions of Iberdrola's Group internal procedure: Procedure for Responding to Incidents Related to Personal Data, which establishes the organization and action criteria for the detection, containment, risk assessment, communication and notification of security incidents in which personal data are involved.

This procedure establishes the obligation of the Group Companies that have been affected by a Personal Data Security Breach related to personal data transferred from the E.E.A, to notify, without undue delay, the Group Companies that they accept liability for any breach of the BCRs occasioned by any of the Group Companies established outside the E.E.A, as well as to the Global Corporate Security Data Protection Coordinator.

In the event that the Personal Data Security Breach is likely to constitute a risk to the rights and freedoms of Data Subjects, the Local Corporate Security Data Protection Coordinator, or where applicable, the Global Corporate Security Data Protection Coordinator shall notify the competent Supervisory Authority, no later than 72 hours after becoming aware of the breach.

Where the Personal Data Security Breach is likely to constitute a high risk to the rights and freedoms of Data Subjects, the Group Companies concerned shall notify the Data Subjects directly without undue delay.

Notifications of a Security Breach must be documented and include at a minimum:

- a. The description of the nature of the Security Breach: number of affected Data Subjects, category of affected Data Subjects, approximate number of personal data records affected, etc.
- b. Name and contact details of the Data Protection Officer or other point of contact where more information can be obtained.
- c. Effects and possible consequences of the Security Breach.
- d. Description of the measures taken or proposed to remedy the Security Breach, including, if applicable, the measures taken to mitigate the possible negative effects.

This documentation must be made available to the Spanish Data Protection Agency and any other Supervisory Authority when requested.

### 3.10. Processing carried out by data processors

Group Companies may not contract the services of a service provider that has access to the personal data for which the Company is the Data controller without first ensuring that the Data processor will apply appropriate technical and organisational measures to ensure the protection of the rights and freedoms of the Data Subjects.

A contract or other similar legal act must be signed, binding the Data processor to the Data controller and establishing the subject matter, 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 Data controller and the Data processor. The obligations of the Data processor shall be, as a minimum and expressly provided for in the contract or similar legal act, the following:

- a. Process the personal data only on documented instructions from the Data controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest

- b. Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. Take all necessary measures to ensure the safety of the treatments.
- d. Not to allow access to personal data to another Data processor without the prior written authorisation, specific or general, of the Data controller. In any case, the processing of personal data carried out by the new subprocessor must comply with the instructions of the controller, and the processor must enter into a contract with the new subprocessor in accordance with the provisions of Article 28 of the GDPR.
- e. Assist the Data controller, taking into account the nature of the processing, through appropriate technical and organisational measures, whenever possible, so that the latter can comply with its obligation to respond to requests aimed at exercising the rights of Data Subjects.
- f. To assist the controller in ensuring compliance with the obligations set out in the GDPR, taking into account the nature of the processing and the information available to the Data processor:
  - Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
  - The Data processor shall notify the Data controller of breaches of the security of personal data without undue delay from the date of becoming aware of such delay
  - The Data processor shall provide reasonable support to the Data controller when conducting any Data Protection Impact Assessment, and in prior consultations with Supervisory Authorities or other competent data protection authorities, where appropriate.
- g. At the choice of the Data controller, delete or return all personal data to the Data controller after the end of the provision of processing services, and delete existing copies unless Union or Member State law requires storage of the personal data.
- h. Make available to the Data controller all information necessary to demonstrate compliance with the obligations applicable to the Data processor, as well as to enable and contribute to the performance of audits, including inspections, by the Data controller or another auditor authorised by the Data controller.
- i. Immediately inform the Data controller in the event of a breach of its obligations as a Data processor.

### 3.11. International processing of personal data

The processing of personal involving a transfer of data to Data controllers and Data processors that are not part of Iberdrola's Group and are located in countries outside the E.E.A must be subject to additional guarantees that ensure that the level of protection is adequate. Therefore, the transfer of personal data from a Group Company to non-adherent Group Companies or to third parties may only take place:

1. When the countries in which the recipient companies (Group Companies 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 referred to in paragraph 1), the Data controller or processor shall take appropriate measures to compensate for the lack of data protection in the destination country. By way of example:



- Standard data protection clauses adopted by the European Commission or by a Supervisory Authority;
- Binding corporate rules for Data processors;
- Binding codes of conduct setting out the obligations of member companies in relation to the international transfer of data in accordance with the GDPR; along with binding and enforceable commitments on the controller or processor of the third country to apply appropriate safeguards, including those relating to the rights of Data Subjects.
- Certification that demonstrates that the certified companies comply with the GDPR in relation to international transfers; along with binding and enforceable commitments on the controller or processor of the third country to apply appropriate safeguards, including those relating to the rights of Data Subjects.
- Legally binding and enforceable instruments between public authorities or bodies.

Apart from the cases provided for in the two previous sections, international data transfers may only be carried out by Group Companies to non-member Group Companies or to third parties if:

- The Data Subject has given his or her explicit and informed consent.
- The international transfer is necessary for (i) the conclusion or performance of a contract between the Data Subject and the controller or for the execution of pre-contractual measures adopted at the request of the Data Subject; (ii) the conclusion or performance of a contract, in the interest of the Data Subject, between the controller and another natural or legal person; (iii) the protection of the vital interests of the Data Subject or other persons, where the Data Subject is physically or legally incapable of giving consent; or (iv) the assertion, exercise or defense of 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 controller or the Data processor and the controller, processor or recipient of the personal data in the third country.
- The international transfer is based on a legitimate interest of the Data controller over which the interests or fundamental rights and freedoms of the Data Subject do not prevail, and also that it is (i) non-repetitive, and (ii) affects a limited number of people, and (iii) specific and appropriate data protection guarantees are adopted. It will also be necessary to inform the Supervisory Authority and the Data Subject. This case is only admissible in exceptional circumstances and when none of the three previous reasons for the transfer are applicable.

The international transfer of data as a result of the provision of services shall not exempt the obligation to enter into a contract with the Data processor in accordance with the provisions of the GDPR

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

### 3.12. Record of processing activities

Each Data controller and Data processor keeps a Record of Processing Activities, which will be documented in writing, including in electronic format, and will include all personal data processing activities they carry out. The Record of Processing Activities will be made available to the supervisory authority upon request.

The Record of Processing Activities must include:

- 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.

- c. A description of the categories of Data Subjects and categories of personal data.
- d. The categories of recipients to whom the personal data is disclosed, including recipients in third countries.
- e. Where applicable, transfers of personal data to a third country, including the identification of such third country or international organisation and in the case of transfers referred to in section 3.11.
- f. The envisaged time limits for erasure of the different categories of data.
- g. A general description of the technical and organisational measures implemented to protect personal data.
- h. The identification of the data processors, both internal and external.

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

- a. The name and contact details of the processor(s) and of 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. International transfers of personal data to a third country or international organisation, including the identification of such third country or international organisation, and in the case of transfers referred to in section 3.11, the documentation of appropriate safeguards.
- d. A general description of the technical and organizational security measures you are implementing.

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

No processing activities that may compromise the rights and freedoms of Data Subjects will be carried out. To this end, and in accordance with the GDPR, an objective analysis of the risks of each processing will be carried out, as described in the following clause.

### 3.13. Objective privacy risk assessment and data protection impact assessment (DPIA)

Processing activities falling within the scope of these BCRs must be subject to an objective privacy risk assessment. In cases where it is found that there is a high risk to the rights and freedoms of Data Subjects, a Data Protection Impact Assessment (hereinafter, "DPIA") will be carried out. In the event that the DPIA shows that the processing entails 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 consists of a more exhaustive analysis of the risks associated with a processing activity, which allows the identification of the mitigating measures of the same, through:

- a. The assessment of threats and vulnerabilities, both legal and technological, including their likelihood and potential impact;
- b. Obtaining the inherent risk;
- c. The assessment of the degree of maturity of safeguards;
- d. Obtaining residual risk;
- e. Implementation of the Action Plan.



### 3.14. Data protection by design and by default

The Data Controller, both at the time of determining the means of processing and at the time of the processing itself, implements appropriate technical and organisational measures, in order to meet the requirements of the GDPR and the BCRs, and protect the rights and freedoms of Data Subjects.

The Data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for the specific purposes of the processing are processed.

Before starting a new processing, activity or modifying an existing one, the legal and technical requirements that are required and necessary must be analysed in order to determine whether the processing by Iberdrola's Group is viable in accordance with the GDPR, following Iberdrola's Group internal procedure, known as the Procedure to guarantee data protection by design and by default.

---

## 4. DATA SUBJECTS RIGHTS

---

With regard to the processing of personal data, the Group Companies guarantee the following inalienable rights to the Data Subjects:

- a. Right of Access, which involves providing information about the personal data held concerning a Data Subject.
- b. Right to Rectification, by virtue of which the Data Subject may request the rectification of inaccurate or incomplete personal data concerning him or her.
- c. Right to Erasure or "right to be forgotten", by which the Data Subject may request the deletion of its personal when the circumstances provided for in the GDPR apply.
- d. Right to Restriction of the Processing, by virtue of which the Data Subject may request the restriction of processing when the circumstances provided for in the GDPR apply.
- e. The right to Data Portability, whereby the Data Subject may receive the personal data concerning him or her, which he or she has provided to a Data controller, in a structured format, and to transmit them to another Data controller.
- f. Right to Object, by which the Data Subject may object to the processing of its personal data for a specific purpose.
- g. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on Data Subjects or similarly significantly affects them.
- h. Right to receive notification regarding rectification or erasure of personal data or restriction of processing.

The Group Companies will only make decisions based solely on automated processing, including profiling, that produces legal effects on the Data Subject or significantly affects him/her, if any of the following conditions are met:

- It is necessary for entering into, or performance of, a contract between the Data Subject and a Group Company Data controller.
- It is authorised by the regulations applicable to the Data controller which also lay down suitable measures to safeguard rights and freedoms and legitimate interests.
- It is based on the Data Subject's explicit consent.

In the first and third case, the Data Subject will be facilitated, at least, with the right to obtain human intervention on the part of the Data controller, to express his or her point of view and to contest the decision.

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

## 5. THIRD PARTY BENEFICIARIES' RIGHTS

The Group Companies shall guarantee that Data Subjects can exercise their rights as third-party beneficiaries under these BCRs. Data Subjects may invoke the rights set out in sections 3, 4, 7, 10, 11, 12 and 13 of these BCRs, which correspond to them as third-party beneficiaries in relation to the processing of their data, under the terms provided in this section. Data Subjects also have the right to easily access these BCRs.

Data Subjects whose personal data is collected and/or processed in the E.E.A by a Group Company (Exporter) and transferred to a Group Company outside the E.E.A (Importer) shall have the right to enforce these BCRs as third-party beneficiaries.

For this purpose:

- **They may lodge a complaint with the competent Supervisory Authority** (at their choice, the E.E.A Supervisory Authority corresponding to their country of residence, place of work or place of alleged infringement) **and before the competent court of the E.E.A.** (at your choice, those of the country of the E.E.A in which the Group Company has an establishment, or those of the country in which the Data Subject has its residence). Likewise, Data Subjects may be represented by a non-profit body, organisation or association under the conditions established in article 80.1 of the GDPR.
- If the Group Company that has allegedly breach the BCRs is established outside the E.E.A, the Data Subject may, under the terms provided for in the previous section, **exercise its rights and lodge a claim**, in accordance with the liability scheme defined in section 12 of these BCRs, against the Group Company that assumes liability in the event of a breach of the BCRs on the side of the Group Company domiciled outside the E.E.A., which shall be considered liable for the infringement. For this purpose, the breach will be deemed to have occurred at the registered office of the Group Company that assumes responsibility.
- Likewise, the Group Company which, in accordance with the liability scheme defined in section 12 of these BCRs, assumes liability in case of a breach of the BCRs on the side of the Group Company domiciled outside the E.E.A, will be **liable for assume any damages suffered by any Data Subject** as a result of a breach of these BCRs by the Group Company or another data importing company, provided that such liability has been declared by a court or other competent authority.

In order to identify the company to which the Data Subject should address his/her claim and which is responsible for a breach of the BCRs, the Data Subject should contact the Global Corporate Security Data Protection Coordinator, whose contact details are: [dpo@iberdrola.com](mailto:dpo@iberdrola.com), who will provide the information about the Responsible Company.

For the abovementioned purposes, these BCRs are constantly available and easily accessible by interested parties through their publication on the website [www.iberdrola.com](http://www.iberdrola.com).

## 6. Training programme

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

All Group Companies employees must complete 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 the collection of such data or in the development of tools used for its processing.

Annex II of the BCRs includes the training requirements for the Group employees regarding personal data protection with a particular emphasis on the BCRs as a transfer mechanism between the Group Companies.

---

## 7. Internal complaints handling procedure

---

Data Subjects may contact the Global Corporate Security Data Protection Coordinator at any time, who is responsible for handling and processing complaints regarding the breach of the BCRs by a Group Company and exercises its functions independently. The Group Companies must comply with the complaints handling procedure included as Annex III of the BCRs.

Upon submission of a claim, an acknowledgment of receipt will be issued. The claim will be resolved within one month of its receipt. This period may be extended by up to two months, depending on the complexity and number of requests received.

In the event that a claim leads to an investigation by the competent Supervisory Authority, the affected Group Company will abide by the decision issued.

---

## 8. Audit and supervision programme

---

The privacy audit programme of the Group Companies expressly includes the verification of compliance with these BCRs, being the verification mechanisms defined in Iberdrola's Group internal procedure called GDPR Compliance Assessment Model. The BCRs Audit Procedure is described in Annex IV.

The Global Corporate Security Data Protection Coordinator determines the scope of the BCRs audit, which includes all aspects of the BCRs, as well as the designation of the internal staff responsible for conducting it and the methods and action plans to ensure that corrective actions are carried out.

The BCRs audit may be conducted internally or through an external audit. The audit report must be communicated to the Board of Directors of the Group Companies responsible in case of BCRs non-compliance, their Local Corporate Security Data Protection Coordinator, and the Global Corporate Security Data Protection Coordinator, specifying the corrective measures, recommendations and a deadline for their implementation.

The BCRs audit is conducted annually. The Board of Directors of the Group Companies in the event of non-compliance with the BCRs may also request the performance of an audit of the BCRs. In addition to the audits carried out on an annual basis, specific audits (ad hoc audits) may be requested by the Global Corporate Security Data Protection Coordinator.

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

The Group Companies must comply with the recommendations on the scope and compliance with these BCRs that may be issued by the data protection authorities.

## 9. COMPLIANCE

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

The Group Companies undertake the following:

- Not to carry out any transfer of data to another Group Company, unless said company is adhered to the BCRs and has mechanisms in place to ensure compliance.
- When acting as a Data Importer, to inform the Data Exporter as soon as possible in the event that, for any reason, including the situations described in paragraph 11, it is unable to comply with the BCRs.
- When acting as a Data Exporter, to suspend the data transfer in the event that the Data Importer fails or is unable to comply with the BCRs.
- When acting as a Data Importer, at the Data Exporter's choice, to delete or return the transferred personal data or any copy thereof when:
  - the Data Exporter has suspended the transfer and compliance with the BCRs cannot be restored within a reasonable time and in any event within one month from the suspension;
  - the Data Importer materially or repeatedly fails to comply with the BCRs; or
  - the Data Importer fails to comply with a binding decision of a court or Supervisory Authority regarding the obligations contemplated in the BCRs.

The Data Importer shall certify the deletion of the personal data to the Data Exporter. Until this action is carried out, the Data Importer shall continue to ensure compliance with the BCRs. If local laws applicable to the Data Importer prohibit the return or deletion of the received personal data, the Data Importer shall continue to comply with the BCRs and will process the data only within the limits permitted by local laws.

Annex V provides information on the operating structure, coordination mechanisms and responsibilities of the Iberdrola's Group Privacy team, which guarantees compliance with the protection of personal data throughout the Group and the absence of conflicts of interest in the performance of duties.

## 10. MUTUAL ASSISTANCE AND COOPERATION DUTY WITH DATA PROTECTION AUTHORITIES

The Group Companies commit to cooperate and assist each other in the event of complaints from a Data Subject or investigations and requests made by the Supervisory Authorities concerning breaches of the BCRs.

The Group Companies also commit to cooperate with the competent Data Protection Authorities within the scope of application of the BCRs and will respond to requests made by such Authorities in relation to the BCRs in the corresponding manner and time frame, and they will abide by the decisions and recommendations issued by these Authorities. To this end, they will follow the Procedure for cooperation with the Supervisory Authorities detailed in Annex VI.

The Group Companies agree to submit to the data protection audits carried out by the Data Protection Authorities.

Any conflict relating to the exercise of the Supervisory Authorities powers in relation to the supervision and enforcement of the BCRs shall be settled by the courts of the Member State to which the Supervisory Authority concerned belongs, in accordance with the procedural laws of that Member State. The Group Companies agree to submit to the jurisdiction of such courts.



## 11. RELATIONSHIP BETWEEN BCRs AND LOCAL LEGAL REGULATIONS

The Group Companies must comply with the applicable local data protection regulations, without prejudice to compliance with these BCRs, provided that the BCRs offer a higher level of protection than that established in local regulations. In all aspects covered by these BCRs where the applicable local legislation establishes a higher level of protection, the local legislation shall.

- **Transfer Impact Assessment: Third Country Regulations and Practices**

The Group Companies will use the BCRs as a tool for international data transfers only after assessing that the local regulations and practices of the destination country applicable to the processing of the data, including data disclosure requirements or any authorisation of access to the data by public authorities, do not impede compliance with the Data Importer's obligations under the BCRs.

In particular, the Group Companies will assess whether the local regulations and practices of the destination country essentially respect fundamental rights and freedoms, and whether the legislative measures contemplated therein are necessary and proportionate in a democratic society to safeguard the legal rights of Article 23.1 of the GDPR.

When assessing local regulations and practices in the third country, which may have implications for compliance with the obligations and commitments set out in the BCRs, the Group Companies shall take into account:

- The specific circumstances of the transfer or set of transfers and subsequent transfers envisaged within the third country or to another third country, including the purposes of the transfer, type of entities involved, economic sector affected by the transfer, categories and format of the personal data transferred, location of processing and storage and transmission channels used.
- The relevant local regulations and practices of the third country, taking into account the circumstances of the transfer, including those that provide for the disclosure of data to public authorities or that authorise access to it, as well as those that regulate access to Personal Data during transmission between the country of the Data Exporter and the Data Importer, together with any applicable limitations and warranties.
- All contractual, technical or organisational safeguards put in place to complement the BCRs safeguards, including measures applied during the transmission and processing of Personal Data in the destination country.

In the event that the Group Companies decide to adopt additional guarantees to those contained in the BCRs, they must inform the Global Corporate Security Data Protection Coordinator and involve him in the assessment carried out.

The Group Companies shall document the assessments of the regulations and practices of the destination country, as well as the additional safeguards adopted and implemented. Such evidence shall be made available to the competent Supervisory Authority.

In the event that the Data Importer is subject, or has reason to believe that it is subject, to regulations or practices, including legislative changes of the third country or requests for access to data, which prevent it or may prevent it from complying with the BCRs, it shall notify the Data Exporter and the Group Companies of this circumstance.

After reviewing the above notification, the Data Exporter, in conjunction with the Global Corporate Security Data Protection Coordinator, will identify additional measures, technical or organizational, to ensure the security and confidentiality of the data. Such measures will be implemented by the Data Exporter and/or Importer. The same applies if a Group Company acting as a Data Exporter has reason to believe that another Group Company acting as a Data Importer is unable to comply with the BCRs.

However, if the Data Exporter, together with the Global Corporate Security Data Protection Coordinator, determines that the BCRs, even having implemented additional measures, cannot be complied with for a particular transfer or set of transfers, or if the competent Supervisory Authorities so deem appropriate, the transfer or set of transfers in question shall be suspended, as well as all those for which the evaluation and reasoning carried out would lead to a similar conclusion, until compliance with the BCRs is again guaranteed or the transfer is terminated.

In the event that one month has elapsed since the suspension of the transfer without it being possible to resume the transfer by ensuring compliance with the BCRs, the Data Exporter shall terminate the transfer or set of transfers. The personal data that have been transferred prior to the aforementioned suspension, and any copies thereof, must be returned in full to the Data Exporter adhering to the BCRs or destroyed, at the latter's option.

The Global Corporate Security Data Protection Coordinator shall inform all Group Companies of the transfer impact assessment carried out and its results, so that the additional guarantees or measures adopted may be applied to similar transfers, or in the event that, even having adopted additional measures, the transfer does not comply with the BCRs, are suspended or terminated.

Finally, the Data Exporter, in collaboration with other importers if necessary, shall carry out continuous monitoring to detect any developments in the third countries to which data are transferred, which may influence the outcome of the initial assessment of the impact of the transfer.

- Regulatory conflict:

In the event of a conflict between the applicable local regulations and these BCRs, such that it is not possible to adequately comply with the latter or that it has a substantial effect on the guarantees provided in the BCRs, the affected Group Company must inform the Global Corporate Security Data Protection Coordinator as soon as it becomes aware of such conflict.

The Global Corporate Security Data Protection Coordinator, upon receipt of the appropriate communication, will document the conflict and will promptly inform the Company and the Group Companies that have previously transferred data to the Group Company raising the conflict.

The Local Corporate Security Data Protection Coordinator will notify the competent E.E.A Supervisory Authority of the conflict and, together with the involved Group Company, will promote the solution that is most compatible with the principles of the GDPR.

When the conflict arises with the applicable regulations of a third country, the competent E.E.A Supervisory Authority will be informed. In the event that the company has been required to disclose data, the communication will include information about the data requested, the requesting body and the legal basis for the disclosure.

In the event that notification to the competent E.E.A Supervisory Authority is prohibited, the requested Group Company shall make every effort to overcome such prohibition and will demonstrate that it has done so. If, despite this, the requested Group Company cannot notify the competent E.E.A Supervisory Authority, it commits to providing annual general information regarding the requests it has received.

Transfers of personal data from a Group Company to any Public Authority cannot be massive, disproportionate or indiscriminate.

---

## 12. LIABILITY

---

In terms of liability, Iberdrola Group designates the following Group Companies as Liable companies ("**Liable Companies**") that agree to assume liability for any breach of the BCRs on the side of the Group Companies domiciled outside the E.E.A:



- Iberdrola España, S.A. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is any company domiciled in Spain that is dependent on it. Likewise, Iberdrola España, S.A. (Single-Member Company) will assume liability for any breach of the BCRs when the entity exporting the data is Iberdrola S.A., as well as any entity, directly or indirectly owned by Iberdrola, S.A., that is not dependent on any of the companies indicated in the following paragraphs as Responsible Companies.
- Iberdrola Participaciones, S.A. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is a subsidiary of it located in any country of the E.E.A.
- Iberdrola Energía Internacional, S.A. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is any company dependent on it located in any country of the E.E.A.

Responsible Society	Exporting entity
Iberdrola España, S.A.(1)	Group company dependent on Iberdrola España, S.A. and located in Spain (*)
	Iberdrola, S.A.
Iberdrola Participaciones, S.A.(2)	Any Group Company, directly or indirectly owned by Iberdrola, S.A. that is not dependent on any of the companies (2) or (3) (*)
	Company of the Group dependent on Iberdrola Participaciones, and located in any country of the E.E.E. S.A. (*)
Iberdrola Energía Internacional, S.A.(3)	Company of the Group dependent on Iberdrola Energía Internacional, S.L. and located in any country of the E.E.E. S.A. (*)

(\*) Annex I contains the Group Companies that are members of the BCRs, grouped by the Group Companies that directly or indirectly control the former.

Likewise, and as an additional safeguard of the commitment undertaken under this clause concerning liability, Iberdrola and the Group Companies possess sufficient assets or have adopted appropriate measures to ensure their ability to compensate for any damages that may result from a breach of these BCRs.

In any case, complaints for breaches of the BCRs by a Group Company may be submitted by the Data Subject in writing to the Global Corporate Security Data Protection Coordinator, whose contact details are: [dpo@iberdrola.com](mailto:dpo@iberdrola.com), or to Iberdrola - Calle Tomás Redondo 1 Madrid -28033- Spain as described in **Annex III - Complaints Handling Procedure**.

The Liable Companies agree to:

- Ensure that the Data Subject has rights and remedies against them before the courts or other competent authorities in the EU that have jurisdiction in accordance with section 5 of these BCRs, as if the violation had been caused by them in the Member State where they are established, instead of by the Group Company outside the E.E.A that has committed the breach.
- Pay compensation for any material or immaterial damage resulting from the breach of the BCRs by the Group Companies.
- Bear the burden of proof to demonstrate that the Group Company outside the E.E.A is not liable for any breach of the rules from which a claim for damages has arisen by a Data Subject.
- Agree to take the necessary measures to remedy breaches of the BCRs of other Group Companies.

---

## 13. UPDATE AND MODIFICATIONS OF THE BCRs

---

The modification and/or update of these BCRs will be carried out in accordance with the provisions set forth in the Procedure for updating the Binding Corporate Rules included in Annex VII, which sets out the process for approving changes to the BCRs and how changes to the BCRs are communicated to the Data Protection Authorities, the Group Companies and to the Data Subjects.

In addition, Iberdrola's Group plans to update the Group's Cybersecurity Framework and the internal procedures referenced in these BCRs on an annual basis.

---

## 14. TERMINATION OF THE BCRs

---

In the event of termination of the IA, the obligations relating to the rights of third-party beneficiaries concerning any personal data within the scope of these BCRs that was transferred from the E.E.A prior to the effective date of termination will remain in force.

In the event that a Group Company, as a Data Importer, ceases to be part of the BCRs, it must delete or return the personal data received under the BCRs. However, if the Data Exporter and the Data Importer agree that the latter may retain the personal data, the provisions of Chapter V of the GDPR must be observed.

---

## 15. CONTACT

---

Data Subjects may address their complaints relating this BCRs, their rights recognized under them or any other matter related to personal data protection to the Global Corporate Security Data Protection Coordinator whose contact details are: [dpo@iberdrola.com](mailto:dpo@iberdrola.com).

If Data Subjects do not agree with the form in which the Group Companies process their personal data, the Complaints Handling Procedure included in Annex III will be utilized.



# Annexes

---

## ANNEX I – *List of the companies included in the scope of the binding corporate rules*

---

The list of Iberdrola's Group companies bounded by these BCRs is available on Iberdrola's website ([www.iberdrola.com](http://www.iberdrola.com)) and can be accessed through the following link: [List of companies included within the scope of the BCRs](#). In this list, the first column reflects the corporate name of each Company, with bold font indicating those companies that directly or indirectly control the ones listed beneath them. The second column reflects the registered office of each company.

---

## ANNEX II - *Training in personal data protection*

---

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

The Global Corporate Security Data Protection Coordinator is responsible for defining the training needs relating data protection within Iberdrola Group and, therefore, will 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. Training and Human Resources Development departments in each country are responsible for the preparation and monitoring of the training plans for the Group's workforce, which includes 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 company's social representation.

Each Training and Human Resource Development Department is responsible for ensuring that the training programme is complied with by all employees and informs the respective Human Resources management of its effective compliance.

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

The training will be conducted *online*, keeping in any case documentary evidence of the details of the training activity carried out, and a record of the employees who have carried it out. For each training, a test will be carried out on the knowledge acquired. If the test is not passed, new ones must be taken until it is passed.

There will therefore be a record of the training action given, recording the dates of its duration, start and end, content of the course, and name of the attendees. The latest version of the course will also be kept on the Iberdrola Intranet.

In accordance with the above, Iberdrola's Group has an annual training programme in personal data protection, designed based on the risks identified in the protection of personal data in the sector for all employees of the Group Companies (inside and outside the E.E.A). Through this training, the necessary measures are adopted to ensure that employees are aware of the requirements derived from the regulations on the protection of personal data and the BCRs, in strict compliance with their obligations regarding the training of employees.

### Annual training programme in personal data protection

#### General training in personal data protection

All employees of the Group Companies must take the general training programme on personal data protection on an annual basis. In addition, employees receive training on other internal procedures, including those related to handling requests for access to personal data by public authorities, and rules relating to both the protection of personal data in general and BCR in particular.



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

The general training in personal data protection deals with the national and international legal framework on personal data protection, internal personal data protection policies, protocols, review of practical cases and privacy and security procedures that must be complied with at Iberdrola.

The purpose of the general training programme on personal data protection is for all employees to understand the basic principles of personal data protection, confidentiality and information security and Iberdrola's privacy and information security policies and procedures.

### **Training in binding corporate rules**

All employees of the Group Companies must complete Iberdrola's BCRs training programme annually.

#### **The BCR training is about:**

1. Concept
2. Binding Corporate Rules of Iberdrola Group
3. Effectiveness, binding nature and consequences of non-compliance

In view of the roles and responsibilities of employees, specific training will be provided on the protocols for updating, filling claims and auditing Iberdrola's BCRs.

---

## **ANNEX III – Complaints handling procedure**

---

Below is the procedure for handling complaints that a Data Subject may submit to Iberdrola Group regarding the processing of their personal data in accordance with the BCRs.

### **Complaint submission**

Complaints regarding the non-compliance of the BCR by a Group Company can be submitted by the Data Subject to the Global Corporate Security Data Protection Coordinator by email to: [dpo@iberdrola.com](mailto:dpo@iberdrola.com) or by post at: Iberdrola Calle Tomás Redondo 1, Madrid -28033- Spain.

### **Complaint management**

The Global Corporate Security Data Protection Coordinator will be responsible for responding to complaints concerning BCR non-compliance by the Group Companies.

Upon receiving a complaint, the Coordinator will acknowledge receipt and assess whether it meets the formal requirements for acceptance. Subsequently, the Coordinator will contact the Local Data Protection Coordinators associated with the case, who will be responsible for providing the necessary information to resolve the complaint.

The Global Corporate Security Data Protection Coordinator will coordinate the response to the interested party, and the complaint will be resolved within one month of receipt. This period may be extended by a maximum of two months depending on the complexity and number of requests received. In such cases, the complainant will be informed within a reasonable timeframe and, in any event, no later than 15 days from the submission of the complaint and provided with an explanation. Additionally, the individual will be notified of the consequences in the event that the complaint is denied or justified.

Data Subjects may contact the Global Corporate Security Data Protection Coordinator at any time, as it is competent to address and process complaints about BCRs non-compliance by any Group Company and exercises its functions independently.

### **Other complaints channels**

The Data Subject shall have the right to enforce compliance with these BCRs by filing a complaint with a Supervisory Authority or by taking legal actions before the Courts, without the need to have exhausted the internal remedies provided for in the previous paragraph. For these purposes:

- They may lodge a complaint before the competent Supervisory Authority (either the one in the relevant E.E.A country of their residence, workplace or where the alleged infringement occurred) and before the competent court in the E.E.A (choosing those of the country where the Group Company has an establishment or those of the country in which the Data Subject has his residence).

In the event that a complaint gives rise to an investigation by the competent Supervisory Authority, the Group Company concerned shall respect the decision adopted.

- In the event that the Group Company that has allegedly failed to comply with the BCRs is established outside the E.E.A, the Data Subject may, under the terms provided for in the previous section, exercise its rights and file its claims in accordance with the liability scheme defined in the BCRs against the Group Company that assumes liability in the event of non-compliance with the BCRs by any of the Companies of the Group domiciled outside the E.E.A, who will be held liable for the infringement. For these purposes, the breach will be understood to have occurred at the registered office of the Group Company that assumes responsibility.
- Likewise, the Group Company which, in accordance with the liability scheme defined in the BCRs, assumes liability in the event of non-compliance with the BCRs by any of the Group Companies domiciled outside the E.E.A, shall assume civil liability for damages suffered by any Data Subject due to 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.

In terms of liability, the Iberdrola Group designates the following Group Companies as Liable companies (“**Liable Companies**”) that agree to assume liability for any breach of the BCRs on the side of the Group Companies domiciled outside the E.E.A:

- Iberdrola España, S.A. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is any company domiciled in Spain dependent on it. Likewise, Iberdrola España, S.A. (Single-Member Company) will assume liability for any breach of the BCR when the entity exporting the data is Iberdrola S.A., and any entity, 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. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is a subsidiary of it located in any country of the E.E.A.
- Iberdrola Energía Internacional, S.A. (Single-Member Company), which will assume liability for any breach of the BCRs when the entity exporting the data is any company dependent on it located in any country of the E.E.A.

The Liable Companies agree to:

- Ensure that the Data Subject has rights and remedies against them before the courts or other competent authorities in the EU that have jurisdiction in accordance with section 5 of these BCRs, as if the violation had been caused by them in the Member State where they are established, instead of by the Group Company outside the E.E.A that has committed the breach.
- Pay compensation for any material or immaterial damage resulting from the breach of the BCRs by the Group Companies.
- Bear the burden of proof to demonstrate that the Group Company outside the E.E.A is not liable for any breach of the rules from which a claim for damages has arisen by a Data Subject.
- Agree to take the necessary measures to remedy breaches of the BCRs of other Group Companies.



---

## ANNEX IV – BCRs audit procedure

---

The internal procedural document of Iberdrola's Group that clearly establishes the verification mechanisms is the Compliance Assessment Model – European Data Protection Regulation. This verification programme is implemented based on Iberdrola's Group compliance model, applicable to all Group Companies included within the scope of the BCRs, and is founded on five pillars:

- Governance Framework;
- Methodologies and tools: Record of Processing Activities, Risk Analysis and Data Protection Impact Assessments (DPIA);
- Procedures, Standards and Guidelines;
- Security measures;
- Compliance Assessment and Reporting

The verification programme involves the personal data protection officers of the different businesses and corporate areas, as well as the Global and Local Data Protection Coordinators who make up the Iberdrola Group's Privacy Team. Internal and external auditors will also participate.

### Internal auditors

The Global Corporate Security Data Protection Coordinator shall determine the scope of the BCRs audit, including the identification of all aspects that must be assessed to verify compliance with the BCRs, as well as the periodicity with which such assessment must be carried out, in view of its scope. Likewise, the Global Corporate Security Data Protection Coordinator will designate the personnel responsible for carrying out the audits internally, guaranteeing, at all times, the independence of the personnel designated to carry out the audit, as well as that said personnel have the necessary skills and technical knowledge to carry out the audits.

### External auditors

The participation of external auditors in the procedure for verifying compliance with the BCRs shall be governed by the following principles:

- Integrity: auditors must maintain honesty, impartiality, and objectivity in their work, avoiding any conflict of interest that may compromise their professional judgment.
- Professional competence and diligence: auditors shall demonstrate that they possess the knowledge, skills, and experience necessary to conduct the audit competently and diligently, in compliance with applicable professional and technical standards.
- Confidentiality: auditors will respect the confidentiality of the information to which they have access during the audit process, protecting the privacy of Data Subjects and the legitimate interests of the Iberdrola Group.
- Independence: auditors shall maintain independence in the exercise of their function, avoiding compromising their ability to make impartial and objective judgments.
- Sufficient evidence: auditors will support their findings with sufficient evidence to verify compliance with the GDPR and, in particular, with the BCRs.
- Regulatory compliance and quality standards: auditors will rigorously comply with current laws and regulations and provide their services in accordance with the best quality standards.
- Clear and transparent communication: the auditors will communicate clearly and transparently the findings, conclusions and recommendations derived from the audit, providing relevant and understandable information to the Iberdrola Group on the outcome of the audit.
- Respect for the rights and responsibilities of stakeholders: auditors will respect the rights and responsibilities of stakeholders.

### Compliance Assessment

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

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

**The assessment will review the following aspects:**

- The legal instruments enabled to make the BCRs binding at the internal level.
- The guarantees offered by the Group Companies in relation to the rights of third-party beneficiaries.
- Cooperation and assistance actions between the Group Companies in the event of complaints from a Data Subject or investigations and inquiries by the Supervisory Authorities in relation to breaches of the BCRs.
- The actions of cooperation with competent Data Protection Authorities and response to the requests that these Authorities make in relation to the BCRs in the corresponding form and period and the compliance with the decisions and recommendations made by them.
- The management of complaints for non-compliance with the BCRs by one of the Group Companies.
- The protocol for updating and modifying the BCRs.
- The methods used to provide information about BCRs to Data Subjects.
- Compliance with the BCRs training programme.
- Decisions made in relation to mandatory requirements of national laws that conflict with BCRs.
- A review of the BCRs text to ensure alignment with the Data Protection Governance Framework.

**Data Protection Reporting**

On a quarterly basis, a report of data protection indicators is prepared at a local and global level containing certain information categorized by corporate area/business and country, in relation to the BCRs, for example:

- Instances of non-compliance with the BCRs;
- The number of companies adhering to the BCRs;
- The number of requests received from competent supervisory authorities in respect concerning the BCRs.

This report will be submitted to the Global Corporate Security Data Protection Coordinator and to the Boards of Directors of the Group Companies, which bear responsibility in cases of non-compliance with the BCRs, along with their Local Corporate Security Data Protection Coordinator, together with the identification of potential data protection risks, which will be included in the Key Risk Report.

---

## **ANNEX V- Iberdrola's group privacy team**

Below is a description of Iberdrola's Group Privacy Team, composed of data protection professionals whose goal is to ensure compliance with global personal data protection, particularly regarding the BCR.

**Global Operating Structure**

Within the Corporate Security Department of Iberdrola's Group, a **Global Corporate Security Data Protection Coordinator (Global Coordinator)** is appointed, whose responsibilities are:

- Proposing and driving the update of the Global Framework for Personal Data Protection (hereinafter the Global PDP Framework) and the global data protection standards.
- Defining the global data protection management system, which will include, among others, global data protection standards and procedures, as well as corporate methodologies and tools, and promote and supervise its implementation in the Group.
- Defining global security standards applicable to the protection of Personal Data, both in internal processing processes and those of third parties.



- Providing advice, recommendations and clarifications on the content of global standards, methodologies, tools and on the Global PDP Framework.
- Establishing a global compliance assessment and coordination system, to assess the risks of non-compliance and the effectiveness of the Data Protection Policy and the Global PDP Framework and reporting to the Global Cybersecurity Committee and the Compliance Office.
- Acting as the liaison with the Data Protection Supervisory Authority on matters affecting the Group as a whole, with the support of the legal services.
- Coordinating the functions and tasks of the local Data Protection Coordinators in Corporate Security in order to promote the implementation of best practices on data protection and the Group's global strategy.
- Complying with the duties of the Data Protection Officer established in the GDPR and to report to the Board of Directors of Iberdrola, S.A.
- Monitoring and ensuring compliance with the BCRs in a coordinated and homogeneous manner, with the support of Iberdrola's Group global and local Data Protection Coordinators.

The Corporate Security Department is assisted by a **Global Data Protection Coordinator from Legal Services**, who will provide support in the definition of the global governance framework and analysis and definition of regulations and contracts in relation to the transfer of Personal Data within the group, as well as in the development of the rest of its functions.

In addition, the most relevant businesses and corporate areas have appointed a **Global Personal Data Protection Coordinator** in order to ensure the alignment of data protection management systems, in their area of responsibility, with corporate standards and compliance with applicable laws and other regulations, such as and when applicable. to ensure the existence of a Record of Processing Activities, privacy risk assessments, incident notification system, etc., and to serve as a channel for dialogue and support with said business or area at the subholding and head of the business, thereby allowing the implementation of the global strategy in all the Group's Companies and sharing of best practices on the matter.

The different coordinators mentioned are part **of the Global Cybersecurity Committee**, constituted under the Cybersecurity Risk Policy, whose function is to supervise the general state of Cybersecurity and the protection of Personal Data in the Group, facilitate its coordination and assist the Corporate Security Department in the implementation of the measures approved by it. all this, in the terms set out in its Internal Regulations.

### **Operating structure of subholding companies**

The Corporate Security Departments of each of the subholding companies appoint a **Local Corporate Security Data Protection Coordinator** who ensures the implementation in their country of the global strategy on personal data protection, taking into account the particularities of their territory.

The Local Corporate Security Data Protection Coordinator of the Group Companies is responsible for data protection at the local level, fulfilling the functions of the Data Protection Officer set out in the GDPR and reporting to the Board of Directors of the relevant subholding company.

In this regard, the Local Corporate Security Data Protection Coordinator will ensure that there is an appropriate level of coordination with the Global Data Protection Coordinator, in relation to matters relevant data protection issues, including key initiatives, risk indicators, and data protection incidents.

Similarly, the Corporate Security departments of the subholding companies will ensure the local implementation of the global personal data protection strategy, as well as compliance with the applicable rules and regulations, also ensuring coordination between the different business and corporate areas.

These Corporate Security Directorates have set up local Data Protection coordination groups to assist the Local Corporate Security Data Protection Coordinator in the performance of his duties. To this end, the subholding companies also have a **Local Data Protection Coordinator of the Legal Services**

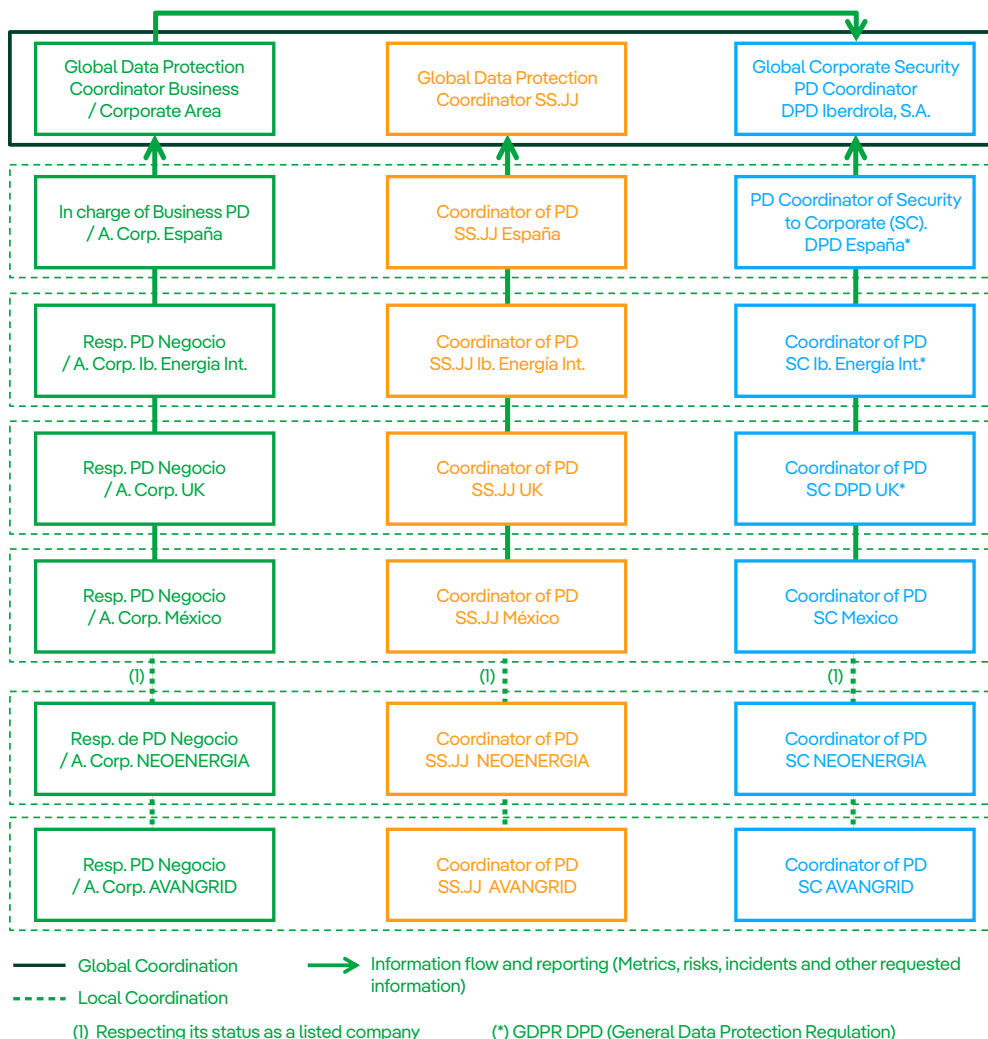
and their respective **Local Data Protection Officers in the relevant businesses and corporate areas**, who assume the corresponding functions and coordinate with their global counterpart. These local coordination groups meet regularly in order to take the necessary measures to ensure the implementation of global guidelines and standards in this area at the local level.

**Coordination mechanisms**

In order to ensure adequate coordination between the Group Companies, in accordance with the Group's corporate structure, the following mechanisms are established:

- **Operational coordination at the local level** between the Local Data Protection Officers of the Business or Corporate Areas, the Local Coordinator of Legal Services and the Local Coordinator of Corporate Security Data Protection, through the local data protection coordination group.
- **Operational coordination at a global level** between the Global Data Protection Coordinators of the Business and Corporate Areas, the Global Data Protection Coordinator of Legal Services and the Global Corporate Security Data Protection Coordinator, through the Global Cybersecurity Committee.
- **Operational coordination at the business or corporate level:** Local Data Protection Coordinators and Officers must report to the relevant Global Data Protection Coordinators on relevant data protection metrics, incidents and risks.

The coordination and **reporting** scheme between the Personal Data Protection Officers in the different Businesses and Corporate Areas, as well as the Data Protection Coordinators, global and local, is reflected below.



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

---

## ***ANNEX VI - Procedure for cooperation with supervisory authorities and other public authorities***

---

Below is the procedure for cooperating with the European Data Protection Authorities regarding Iberdrola's BCRs.

The Group companies commit to collaborate with the European Data Protection Authorities within the scope of the BCRs and will respond appropriately and within the established time frame to any requests made by these Authorities in relation to the BCRs, as well as to comply with the decisions and recommendations made by them. Likewise, the Group Companies accept, if necessary, to undergo on-site inspections by the respective Authorities

In addition, in relation to access requests to personal data addressed to the Data Importer by a Public Authority of the importing country, the Data Importer shall:

- Immediately notify the Data Exporter and, where possible - if necessary with the help of the Exporter - the Data Subject, in the event of:
  - Receiving an access request from a Public Authority, under the laws of the destination country or another third country, for the disclosure of personal data transferred under the BCRs. The notification shall include information about the personal data affected by the request, the requesting authority, the legal basis for the request, and the response provided.
  - Becoming aware of any direct access by a Public Authority, under the laws of the destination country, to the personal data transferred under the BCRs. The notification shall include all available information held by the Data Importer.
- In the event that the laws of the destination country prohibit the notification referred to in the previous point, the Data Importer must make every effort to waive this prohibition and communicate as much information as possible to the Data Exporter as soon as possible. In addition, the Data Importer must document its efforts to evidence them in the event of a possible requirement by the Data Exporter.
- Provide the Data Exporter, on a regular basis, with all relevant information in relation to the access requests received. In particular, number of requests, type of data requested, requesting authorities, whether applications have been challenged and the outcome of such challenges, etc. In the event that the Data Importer is subject to a prohibition on disclosing the aforementioned information, it must notify the Data Exporter of this circumstance immediately.
- Preserve the information communicated to the Data Exporter for as long as the personal data is subject to the safeguards provided by the BCRs and make it available to the competent Supervisory Authorities upon request.
- Assess whether the request for disclosure is lawful, in particular whether the requesting public authority has the power to request disclosure of the data, and challenge or appeal the request if, after the assessment, it is concluded that there are reasonable grounds to deem it unlawful under the law of the country of destination, the applicable obligations of international law and the principles of international comity. If the request is challenged, the Data Importer will seek interim measures in order to suspend the request effects until the competent judicial authority resolves the challenge. It will not disclose the requested personal data until required to do so by the applicable procedural rules.
- Document its assessment on the legality of the request received, as well as any issues related to it and, as far as possible, make such documentation available to the Data Exporter and the competent Control Authorities, if requested.

- Provide as little information as possible when responding to a request for disclosure, based on a reasonable interpretation of that request.

In any case, the transfers of personal data made by a Group Company to any Public Authority may not be massive, disproportionate or indiscriminate, but must be limited to what is strictly necessary.

The Global Corporate Security Data Protection Coordinator shall, upon request, provide access to the results of the BCR audit reports to the competent Supervisory Authorities or European Data Protection Authorities.

In line with the Group's commitment to cooperation and assistance during investigations and queries from the Data Protection Supervisory Authorities in relation to compliance with the BCRs, responses 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 the legal services, will respond to such requests.

---

## **ANNEX VII – Procedure for updating iberdrola's binding corporate rules**

---

Below is the procedure for updating Iberdrola's BCRs, which includes the process for approving changes to the BCRs, as well as how changes are communicated to the Data Protection Authorities, Group Companies and Data Subjects.

### **Modifications to the Binding Corporate Rules**

Modifications to the BCRs include any changes that may affect the level of protection offered by the BCRs or significantly affect the BCRs, for example, legislative changes or changes in the structure of the Group.

Modifications to the BCRs must be approved by the Global Corporate Security Data Protection Coordinator and communicated to the Global Cybersecurity and Data Protection Committee (or the Committee that replaces its functions) for their awareness.

Iberdrola, S.A. will communicate any proposed modification to the BCRs to the Spanish Data Protection Agency within a maximum period of fifteen (15) days, with a brief explanation of the reasons for the modification, in order for the Spanish Data Protection Agency, on one hand, to inform the Supervisory Authorities of such modifications and, on the other hand, within its competence and without prejudice to any observations that other Supervisory Authorities may formulate regarding the proposed changes, to determine whether the proposed modification should undergo the cooperation procedure for the approval of the BCRs. The modification will not be implemented until validated by the Spanish Data Protection Agency

### **Updates to the Binding Corporate Rules**

The BCRs will be updated regularly to reflect the current situation at any given time. The updates to the BCRs, may be due to changes in the list of Group Companies subject to them, the inclusion of recommendations from the European Data Protection Board or other factors.

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

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

The Global Data Protection Coordinator will also notify the Spanish Data Protection Agency annually in the event that there have been no changes to the BCRs, incorporating the confirmation that, in the event that one of the Member Companies must respond for a breach of the BCRs, it has sufficient assets to meet such liability.



Without prejudice to the provisions set forth in this and the previous section, where a modification to the BCR would possibly be detrimental to the level of the protection offered by the BCR or significantly affect them (e.g. changes to the binding character, change of the liable BCR members, it must be communicated in advance to the Supervisory Authorities, via the Spanish Data Protection Agency, with a brief explanation of the reasons for the update. In this case, the Supervisory Authorities will also assess whether the changes made require a new approval.

### **Record of modifications to the Binding Corporate Rules and their communication**

The BCRs are subject to a register of modifications, which records the date of each review and the changes made as a result of such revision. The **Global Corporate Security Data Protection Coordinator** will keep an up-to-date record of the modifications to the BCRs and an updated list of the Group Companies subject to the BCRs and will be responsible for communicating the modifications and updates to the Spanish Data Protection Agency.

The **Global Corporate Security Data Protection Coordinator** will also ensure that any modifications to the BCRs are communicated promptly or without undue delay via direct notification to the Spanish Data Protection Agency, as well as to any other competent Supervisory Authority and to the Group Companies.

Information regarding modifications to the BCRs will be communicated to data subjects by publishing it on IBERDROLA's intranet and corporate website, and by using other means such as general communication.

The **Global Corporate Security Data Protection Coordinator** will ensure that all new Group Companies adhere to the BCRs by signing the relevant adherence agreement and effectively implementing them, before a transfer of personal data is made to them.

The **Global Corporate Security Data Protection Coordinator** shall be responsible for keeping the BCRs up-to-date and complying with the provisions set out in Article 47 of the GDPR.



