

## Personal Data Protection Policy

### 1. Purpose

The purpose of this Policy is to determine the principles and procedures to be followed by all the employees that work at Atlantica Sustainable Infrastructure Plc. or in any of its subsidiaries (hereinafter, 'Atlantica', the 'Group', or the 'Company') in relation to the protection of personal data, guaranteeing, in any case, the compliance of the applicable legislation.

In particular, the purpose of this Policy is to guarantee the personal data protection rights of all natural persons associated to the companies belonging to Atlantica, ensuring that their fundamental rights to honour and personal privacy are observed in the processing of the different kinds of personal data, originating from different sources and for various purposes depending on their business activity.

### 2. Scope of application

The Policy shall be applicable to Atlantica, its directors, managers and employees, as well as to all persons that have any relation with the Group.

In addition, those subsidiaries that are subject to specific local data protection regulations, as well as their respective dependent companies, shall provide the necessary mechanisms to ensure adequate coordination with the rest of the Group in relation to general personal data protection.

In those subsidiaries or entities in which Atlantica has an indirect holding but which are not part of the Group, their representatives shall strive to ensure that the provisions of this Policy are observed and that its principles are applied insofar as possible.

### 3. Principles of personal data processing

This Policy shall be governed by the following principles:

#### a. General principles:

Atlantica and any of its subsidiaries shall strictly comply with the data protection legislation applicable in their jurisdiction, as well as with any regulations relating to the type of personal data processing carried out and with any regulations that apply pursuant to rules or binding agreements endorsed by the Group.

Group companies shall encourage compliance with the principles set forth in this Policy: (i) in the design and implementation of all procedures involving personal data processing; (ii) in any contracts or obligations entered into with natural persons; and (iii) in the implementation of any systems and platforms enabling access by Atlantica professionals, or third parties, to personal data and to the processing of such data.

#### b. Principles regarding personal data processing:

##### i. Principle of lawfulness, fairness and transparency in personal data processing.

Personal data must be processed lawfully, fairly and in a transparent manner, in accordance with the applicable legislation. To this end, personal data must be processed for specific, explicit and

legitimate purposes, in accordance with the applicable legislation. These purposes shall be specified when collecting personal data.

Wherever it should prove mandatory or appropriate pursuant to the applicable legislation, consent must be obtained from the data subjects before collecting such data.

In particular, Atlantica shall not collect or process personal data relating to ethnic or racial origin, political opinions, creed, religious or philosophical beliefs, sexual life or sexual orientation, trade union membership, data concerning health, or genetic or biometric data for the purpose of uniquely identifying a natural person, unless the collection of such data is necessary, legitimate and required or allowed by the applicable legislation, or by internal or business processes that make it necessary, in which case they must be collected and processed according to that set forth in the applicable data protection legislation.

Personal data processing shall be transparent in relation to the data subject, providing them with all the information on the processing of their data in an easily accessible and easy to understand manner, using clear and plain language. It should be transparent to natural persons that their personal data are being processed. Information regarding the processing of personal data shall be made available to the data subject in detail, both regarding the processing itself and the rights of the data subject, and shall comply with all the requirements established by the applicable legislation.

#### **ii. Principle of data minimisation.**

The personal data processed shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Personal data shall only be processed if the purpose of the processing cannot be reasonably fulfilled by other means. Consequently, only the data that is adequate for such a purpose or purposes shall be processed, and the data not necessary for complying with the purposes for which they are processed, shall not be processed.

#### **iii. Principle of accuracy.**

The personal data processed must be accurate and up to date. Otherwise, they must be erased or rectified. Atlantica shall use all measures at its disposal to ensure that the personal data processed are up to date, and if this is not the case, it shall proceed to correct or update said data.

#### **iv. Principle of storage duration limitation.**

Personal data shall not be stored any longer than necessary to fulfil the purpose for which they are processed, except in the cases provided for by law. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

#### **v. Principles of integrity and confidentiality.**

The processing of personal data must ensure, by means of technical and organisational measures, adequate security of the personal data to protect against unauthorised or unlawful processing thereof, and against the accidental loss, destruction or damage of the said data. Atlantica shall

implement internal policies and apply measures that comply, in particular, with the principles of the protection of data by design and by default.

The measures to process the personal data collected and processed by Atlantica must ensure the ongoing confidentiality, integrity, availability and resilience of the systems used to process the said data, and must not be used for any purposes other than those stated to justify and authorise their collection, nor must they be disclosed or transferred to third parties, except in those circumstances in which this is permitted by the applicable legislation. Similarly, processes shall be established for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

#### **vi. Principle of proactive responsibility (accountability).**

Atlantica and any of its subsidiaries shall be accountable for compliance with the principles set forth in this Policy and the requirements established in the applicable legislation and must be able to prove such compliance.

Atlantica and any of its subsidiaries must implement appropriate procedures to its business needs and legal requirements that are approved within the Company in relation to data protection. These include the duty to keep an updated records of processing activities, describing the data processing activities it is carrying out within the framework of its activities, assess the risks associated with its data processing in order to determine the measures that need to be applied to ensure that personal data are processed in accordance with legal requirements, making available to all data subjects information relating to the processing of their personal data; do the verification of suppliers that contact with Atlantica and the duty to store personal data only during the time periods notified by Atlantica.

Among the different activities carried out within Atlantica, special attention must be paid to compliance and supervision with regard to international transfers of personal data; with regard to verification relating to the processing of the personal data of all those suppliers with whom it intends to contract; as well as that proper attention is given to data subjects that exercise their rights.

In the event of an incident causing any accidental or unlawful destruction, loss or alteration of the personal data, or leading to any unauthorised disclosure or access to said data (personal data security breaches), the internal protocols established to this end must be applied. Any such incidents must be recorded and the measures established in the internal protocols prepared for this purpose must be implemented to resolve or mitigate any negative consequences for the data subjects. As soon as they become aware of any personal data security breach, Atlantica personnel shall duly inform the Compliance Committee so that it can study the incident and assess whether it must notify the competent supervisory authorities, as well as the data subjects involved, in the manner and within the time periods established by the applicable legislation.

#### **4. Implementation and responsibilities**

The Compliance Committee shall be responsible for coordinating and managing personal data protection activities in Atlantica. It shall develop and implement, in accordance with the provisions of this Policy and the applicable legislation, Atlantica's internal rules on global data protection

management, compliance of which shall be mandatory for its directors, managers and employees, as well as for all persons that have any relation with Atlantica.

The Compliance Committee shall also establish local internal procedures that implement the principles set forth in this Policy and which specify the content thereof in accordance with the applicable law in their respective jurisdictions.

The IT Department shall be responsible for implementing within Atlantica's information systems the security control measures or developments needed to ensure compliance with the internal rules on global data protection management.

## **5. Control and assessment**

The Compliance Committee is responsible for supervising compliance of the provisions of this Policy.

Regular audits shall be carried out by internal or external auditors in order to verify compliance of this Policy.

*This Policy was approved by the Compliance Committee in December 2020.*