



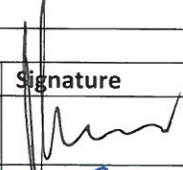



AboitizPower


POLICY

DATA PRIVACY

APC-ERM-004

Revision Details			
Page No.	Revision No.	Description of previous and current revision	Effective Date
All	00	Initial Issue	2017.08.31

Document Approval				
Role	Name	Position	Signature	Date
Prepared by	Ronaldo Ramos	VP – ERM & Data Privacy Officer		8/7/17
Reviewed by	Joseph Trillana Gonzales	FVP – General Counsel		8/8/17
Endorsed by	Luis Miguel Aboitiz	EVP & COO		8 Aug 2017
Approved by	Antonio Moraza	President & COO		8/9/2017

	ABOITIZ POWER CORPORATION	Document Code : APC-ERM-004
		Revision No. : 00
	POLICY DATA PRIVACY	Effective Date : 2017.08.31
		Page 2 of 7

1. PURPOSE

This policy is hereby adopted by the Company to:

- 1.1. Comply with the statutory obligation set forth under the Data Privacy Act and the regulations of the National Privacy Commission, in particular.
- 1.2. Ensure the fair and lawful processing of the personal data of data subjects, including employees, clients, customers, shareholders, and other individuals.
- 1.3. Provide guidelines to team members on the proper handling of personal data.
- 1.4. Ensure the confidentiality, integrity, and availability of personal data under the control of the Company.
- 1.5. Protect the Company from reputational and legal risks that may result from non-compliance with the Data Privacy Act.

2. SCOPE

This policy shall cover all personal data in whatever form (e.g. physical or digital), and processing of personal data in whatever manner (e.g. manual or automated) by the Company, its directors, officers, and employees of the Company.

3. OWNERSHIP

The Aboitiz Power Corporation DPO is responsible for ensuring compliance to this policy.

4. POLICY

4.1. DATA PRIVACY GOVERNANCE

4.1.1. Oversight

The Board of Directors of the Company shall have overall compliance with the Data Privacy Act and implementation of this policy and other related policies of the Company.

4.1.2. Data Privacy Officer

A Data Privacy Office (DPO), who shall be an organic employee of the Company, shall be appointed by the Chief Executive Officer (CEO). The DPO shall report directly to the CEO. In the event that the DPO has other job functions with reporting line to another senior officer, he/she shall have direct reporting line to the CEO for his DPO functions.

The DPO shall have the following duties and responsibilities:

- 4.1.2.1. Ensure the compliance with the Data Privacy Act and regulations, as well as this policy and other related policies of the Company;
- 4.1.2.2. Ensure the regular review (at least annually) of privacy related policies, guidelines, and procedures of the Company;
- 4.1.2.3. Coordinate with the relevant officer/s of the Company responsible for information security management for the effective implementation of information security measures in the Company to ensure the confidentiality, integrity, and availability of personal data;
- 4.1.2.4. Organize privacy and information security trainings;
- 4.1.2.5. Coordinate with the Company's Data Breach Response Team in the management of security incidents and personal data breaches;
- 4.1.2.6. Oversee and coordinate the conduct of privacy impact assessments to identify privacy risks in the Company;
- 4.1.2.7. Develop and implement remediation plans for privacy and information security risks in coordination with the information security officer and process owners;



- 4.1.2.8. Monitor compliance with the Company's privacy and information security standards of third party providers and other entities with access to personal data under the control of the Company; and
- 4.1.2.9. Ensure compliance by the Company of the reportorial, registration, and other regulatory requirements of the National Privacy Commission.

4.1.3. Team Leaders

The team leader of any department, which processes personal data, shall have the following duties and responsibilities:

- 4.1.3.1. Understand the Company's compliance obligations under the Data Privacy Act and related regulations;
- 4.1.3.2. Ensure implementation of policies and guidelines established for compliance with the Data Privacy Act and related regulations, as well as with this policy and other privacy and information security related policies of the Company, by embedding such policies and guidelines in the day-to-day processes and procedures of the department;
- 4.1.3.3. Conduct privacy impact assessments, as may be needed;
- 4.1.3.4. Coordinate with the DPO and the information security officer in the development of controls and mitigation plans to address identified privacy risks.
- 4.1.3.5. Ensure the implementation of risk controls and mitigation plans in the department;
- 4.1.3.6. Promote a culture of privacy in the department;
- 4.1.3.7. Ensure that team members have the capability to comply with privacy and information security requirements as provided by law, regulations, or internal company policies and guidelines; and
- 4.1.3.8. Report immediately to the DPO any security incident or data breach, in accordance with the Company's incident response policy and procedure.

4.1.4. Team Members

Each team member, who processes personal data, shall have the following duties and responsibilities;

- 4.1.4.1. Understand the Company's compliance obligations under the Data Privacy Act and related regulations;
- 4.1.4.2. Understand and comply with privacy and information security policies and procedures in the processing of personal data;
- 4.1.4.3. Report immediately to his/her respective Team Leader any security incident or data breach in accordance with the Company's incident response policy and procedure;
- 4.1.4.4. Implement controls and mitigation plans to address privacy risks; and
- 4.1.4.5. Regularly attend or undergo privacy trainings and other learning activities.

4.2. PROCESSING OF PERSONAL DATA

4.2.1. Rights of a Data Subject

The rights of a data subject, as provided in the Data Privacy Act, should be observed when processing personal data.

- 4.2.1.1. Right to be informed. A data subject has the right to be informed on the following matters:
- 4.2.1.2. Right to object. A data subject has a right to object to processing, which may cause him damage or distress, as well as processing for direct marketing, automated processing, or profiling.
- 4.2.1.3. Right to access. A data subject has the right to reasonable access, upon demand, to the following:
- 4.2.1.4. Right to rectification. The data subject has the right to dispute the inaccuracy or error in their personal data, and have the Company correct it immediately and accordingly, unless the request is vexatious or unreasonable.
- 4.2.1.5. Right to erasure or blocking. A data subject has the right to suspend, withdraw, or order the blocking, removal, or destruction of his personal data from the Company's filing system, upon discovery and substantial proof that the personal data are incomplete, outdated, false,



unlawfully obtained, used for unauthorized purpose, or no longer necessary for the purposes for which they were collected.

4.2.1.6. Right to be indemnified. A data subject has a right to be indemnified for any damages sustained due to inaccurate, incomplete, false, unlawfully obtained, or unauthorized use of personal data.

4.2.1.7. Right to lodge a complaint. A data subject has the right to lodge a complaint before the National Privacy Commission for any violations of his or her rights granted under the Data Privacy Act.

4.2.1.8. Right to data portability. A data subject shall have the right to obtain from the Company a copy of his or her personal data in an electronic or structured format that allows for further use, should his or her personal data be processed in an electronic or structured format subject to the specifications, technical standards, modalities, procedures, and other rules for transfer of such personal data in an electronic or structured format to be issued by the National Privacy Commission.

The foregoing rights may be invoked by the data subject's lawful heirs or assigns, in case of the data subject's death or incapacity.

4.2.2. Data Processing System

To ensure effective privacy compliance and risk management, the Company shall document the following:

4.2.2.1. Departments, employees, or third parties with functions relating to personal data processing.

4.2.2.2. The categories of and inventory of data subjects and the types of personal data being processed.

4.2.2.3. A description of the information flow, from the point of collection up to the disposal of personal data, including any processing done in between, as well as the manner and extent of processing.

4.2.2.4. The purposes for processing, including any intended future processing or data sharing.

4.2.2.5. The recipients or intended recipients of personal data.

4.2.3. Data Collection

4.2.3.1. The data subject must be informed, in clear and plain language, that his personal data is or will be collected and processed. For this purpose, a privacy statement containing the following information shall be supplied to the data subject at the point of collection (e.g. websites, intranet, microsite, mobile apps, and customer and employee forms):

4.2.3.1.1. Description of personal data to be processed;

4.2.3.1.2. Purpose/s of processing;

4.2.3.1.3. Scope and method of processing;

4.2.3.1.4. Parties to whom the personal data may be disclosed;

4.2.3.1.5. Contact details of the Company or its Data Privacy Officer;

4.2.3.1.6. Retention period; and

4.2.3.1.7. His rights as a data subject.

Prior notification to data subject shall be made in case of amendment in privacy statement.

4.2.3.2. Except in instances allowed by law or regulation, the consent of the data subject to processing must be obtained prior to collection. In the case of the processing of sensitive or privileged information, all parties must have given their consent prior to processing.

4.2.4. Fair and Lawful Processing

Processing must be for purposes that are not contrary to law, morals, or public policy. Personal data must not be misused and processing must be in accordance with the declared and specified purposes. Appropriate measures shall be implemented to prevent misuse of personal data that can harm a data subject.

4.2.5. Data Quality

Data quality must be ensured when processing personal data.



- 4.2.5.1. Personal data must be accurate, relevant, and where necessary for purposes for which it is to be used, kept up-to-date.
- 4.2.5.2. Inaccurate or incomplete data must be corrected, supplemented, destroyed, or their further processing restricted.
- 4.2.6. Proportionality of Processing
Processing must be adequate and not excessive, in relation to the purposes for which they are collected and processed.
- 4.2.7. Retention
Personal data shall be retained only for as long as necessary for the fulfillment of the purposes for which it was obtained, or for the establishment, exercise or defense or legal claims, or for legitimate business purposes, or as provided by law.
- 4.2.8. Data Sharing
 - 4.2.8.1. The consent of the data subject on data sharing must be obtained even when the data is to be shared with the Company's parent, subsidiaries, or affiliates.
 - 4.2.8.2. Any data sharing agreement must be covered by a data sharing agreement, which shall provide; among others, the data privacy and security standards to be observed.
- 4.2.9. Security Measures
Taking into account its risk profile, the Company shall implement the appropriate organizational, physical, and technical security measures to ensure privacy and data protection.
 - 4.2.9.1. Promote privacy and data protection awareness in the Company, through trainings and regular communication.
 - 4.2.9.2. Establish proficiency skills development and training for employees handling personal data to ensure protection of personal data. Trainings in data privacy and information security policies and procedures should be part of the on-boarding process for new employees handling personal data.
 - 4.2.9.3. Employees, service providers, and other third parties, who have access to personal data not intended for public disclosure shall be required to hold personal data under strict confidentiality, even after termination of employment or contractual relations. This requirement shall be enforced through confidentiality agreements or confidentiality clauses in service agreements.
 - 4.2.9.4. Information security measures shall be adopted. In this regard, information security management policies are deemed incorporated in this policy.
- 4.2.10. Outsourcing
The Company shall ensure the protection of personal data when outsourcing activities that involve processing of personal data. Among the measures that can be undertaken to ensure data protection by contractors or service providers are the following:
 - 4.2.10.1. Set appropriate privacy and security standards (organizational, physical, and technical measures) to be complied by contractors or service providers when processing personal data.
 - 4.2.10.2. Take into account in the accreditation, hiring, and performance evaluation processes the capability of contractors or service providers to meet the privacy and security standards set by the Company.
 - 4.2.10.3. Embed privacy requirements, security standards, data breach management protocol, and the right of the Company to audit compliance with the foregoing requirements in the agreements with contractors or service providers.

4.3. PERSONAL DATA BREACH MANAGEMENT

- 4.3.1. As part of its information security management system, the Company shall establish detective controls (which, depending on a company's risk profile, may be a combination of process, human capital, physical, and technological controls) to detect potential or actual security incidents or data breaches, as well as complaints, non-compliances, or misconducts relating to privacy and data protection.



- 4.3.2. The Company shall establish and implement a security incident management policy, which shall include the following:
 - 4.3.2.1. Creation of a data breach response team to ensure that timely and appropriate action is taken in the event of a security incident or personal data breach.
 - 4.3.2.2. Implementation of an incident response procedure, including the execution of corrective actions and controls to:
 - 4.3.2.2.1. Contain or mitigate the negative effect of a security incident, data breach, complaint, non-compliance, or misconduct;
 - 4.3.2.2.2. Restore integrity to the information and communications system; and
 - 4.3.2.2.3. Improve prevention and detection of future incidents.
 - 4.3.2.3. The conduct of interval investigation to understand the facts, circumstances, root causes, and appropriate resolution.
 - 4.3.2.4. The procedure for contacting law enforcement authorities, in case possible criminal acts were committed.
 - 4.3.2.5. Compliance with the notification and reporting requirements of the National Privacy Commission, in the event of occurrence of personal data breach or security incident.

4.4. REGISTRATION AND OTHER COMPLIANCE REQUIREMENTS

- 4.4.1. Registration of Data Processing System
 - 4.4.1.1. The Company is required to register its personal data processing system with the National Privacy Commission, if it has at least two hundred-fifty (250) employees.
 - 4.4.1.2. Even if it has less than two hundred-fifty (250) employees, it may nevertheless be required to register its personal data processing system with National Privacy Commission if it carried out processing that:
 - 4.4.1.2.1. Involves the sensitive personal information of at least one thousand (1,000) individuals;
 - 4.4.1.2.2. Is likely to pose a risk to the rights and freedom of a data subject; or
 - 4.4.1.2.3. Is not occasional.
- 4.4.2. Notification of Automated Processing System. The Company is required to notify the National Privacy Commission if:
 - 4.4.2.1. It carries out automated data processing, which becomes the company's sole basis for decision-making about a data subject, and
 - 4.4.2.2. The decision would significantly affect the data subject.
- 4.4.3. Annual Report. A general summary of the security incidents and data breaches hereof shall be submitted to the National Privacy Commission annually, in accordance with its rules.

4.5. DISCIPLINARY ACTION

Violations of this policy, the Data Privacy Act, and its Implementing Rules and Regulations; including data breaches, will be dealt with in accordance with an established disciplinary action and appropriate responses for potential legal actions, including civil and criminal actions.

5. REFERENCES

No references.

6. DEFINITIONS

6.1. Terms

- 6.1.1. Company – Aboitiz Power Corporation
- 6.1.2. Data Subject – An individual whose personal, sensitive personal, or privileged information is processed.



- 6.1.3. Data Processing Systems – Structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including purpose and intended output of the processing.
- 6.1.4. Data Sharing – Disclosure or transfer to another entity of personal data under the custody of a company, and excludes outsourcing, or the disclosure or transfer of personal data by the company to a contractor.
- 6.1.5. Direct Marketing – Communication, by whatever means of any advertising or marketing material, which is directed to particular individuals.
- 6.1.6. Personal Data – All types of personal information, including sensitive personal information and privileged information.
- 6.1.7. Personal Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:
 - 6.1.7.1. An availability breach resulting from loss, accidental, or unlawful destruction of personal data;
 - 6.1.7.2. Integrity breach resulting from alteration of personal data; and/or
 - 6.1.7.3. A confidential breach resulting from the unauthorized disclosure or access to personal data.
- 6.1.8. Personal Information – Any information from which the identity of an individual is apparent or can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual.
- 6.1.9. Processing – Any operation or any set of operations, may be automated or manual, performed upon personal data including the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.
- 6.1.10. Profiling – Any form of automated processing of personal data, consisting of the use of personal data to evaluate certain personal aspects of an individual, in particular to analyze or predict aspects concerning an individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- 6.1.11. Privileged Information – Any and all forms of data considered to be privileged communication under pertinent law, including spousal communication, attorney-client communication, and doctor-patient communication.
- 6.1.12. Security Incident – Event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.
- 6.1.13. Sensitive Personal Information – refers to personal information:
 - 6.1.13.1. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations;
 - 6.1.13.2. About an individual’s health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such an individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
 - 6.1.13.3. Issued by government agencies to an individual, including social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
 - 6.1.13.4. Specifically established by law to be kept classified.