DBP Data Privacy Policy

Introduction

This Data Privacy Policy (the "Policy") is issued in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission (NPC).

It is the policy of the Bank to respect and uphold data privacy rights, and to ensure that all personal data collected from the Bank's data subjects – clients, employees and other third parties - are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality espoused in the Data Privacy Act.

As a repository and processor of personal data, the Bank endeavors to institute fair information practices as part of its commitment to product and service quality that conforms to the expectations of its data subjects.

Objectives

Specifically, this Policy is hereby adopted to:

1. Ensure fair and lawful processing of the personal data of data subjects, including employees, clients, customers, shareholders and other individuals;
2. Ensure the confidentiality, integrity and availability of personal data under the control of the Bank;
3. Protect the Bank from reputational and legal risks that may result from non-compliance with the Data Privacy Act; and
4. Comply with the statutory obligations set forth under the Data Privacy Act and the regulations of the National Privacy Commission (NPC).

Scope

All personnel of the Bank, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Policy.

This policy covers consultants or employees of third parties under a contractual obligation with the Bank (including sub-contracting and outsourcing arrangements).

The Policy applies to all personal data held by the Bank relating to identifiable information of individuals in whatever form (e.g. physical or digital), and the processing of personal data in whatever manner (e.g. manual or automated).

This Policy shall be subject to limitations provided under Section 5 (Special Cases) of the Data Privacy Act's Implementing Rules and Regulations (IRR).

Definition of Terms

The following terms used in this Policy are defined for consistency, uniformity in usage and in accordance with the Data Privacy Act of 2012:

1. **Act**

   The Act refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012.

2. **Bank**

   The Bank shall refer to the Development Bank of the Philippines.

3. **Commission**

   The Commission refers to the National Privacy Commission.

4. **Consent of the data subject**

   Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal data, sensitive personal data and privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

5. **Data subject**

   Data subject refers to an individual whose personal, sensitive personal and/or privileged information is processed and includes the Bank's employees, clients, shareholders, job applicants and other individuals whose personal data is collected by the Bank.

6. **Data processing systems**

   Data processing systems refer to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.

7. **Data sharing**

   Data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing or the disclosure or transfer of personal data by a personal information controller to a personal information processor.

8. **Direct marketing**

   Direct marketing refers to communication by whatever means, of any advertising or marketing material which is directed to a particular individual/s.

9. **Filing system**

   Filing system refers to any set of information relating to a natural or juridical person/s to the extent that, although the information is not processed by any equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to a criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

10. **Information and communications system**

    Information and communications system refers to a system for generating, sending, receiving, storing or otherwise processing of electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted or stored, and any procedure related to the recording, transmission or storage of electronic data, electronic message or electronic document.

11. **Personal data**

    Personal data refers to all types of personal information.

12. **Personal data breach**

    Personal data breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to the personal data transmitted, stored or otherwise processed.

13. **Personal information**

    Personal information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information or when put together with other information would directly and certainly identify an individual.

14. **Personal information controller**

    Personal information controller refers to any natural or juridical person, or any other body who controls the processing of personal data or instructs another to process personal data on its behalf. The term excludes:

    a. A natural or juridical person or any other body, who performs such functions as instructed by another person or organization; or

b. A natural person who processes personal data in connection with his or her personal, family or household affairs.

There is control if the natural or juridical person or any other body decides on what information is collected or the purpose or extent of its processing.

15. **Personal information processor**

Personal information processor refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.

16. **Processing**

Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking and erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system.

17. **Profiling**

Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

18. **Privileged information**

Privileged information refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

19. **Public authority**

Public authority refers to any government entity created by the Philippine Constitution and all relevant laws, vested with law enforcement or regulatory authority and functions.

20. **Security incident**

Security incident is an event or occurrence that affects or tends to affect data protection, or that which 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.

21. **Sensitive personal information**

Sensitive personal information refers to:

a. an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;
b. an individual's health, education, genetic, sexual life, or proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings or the sentence of any court in such proceedings;
c. information issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
d. information specifically established by an executive order or an act of Congress to be kept classified.

I. POLICIES

The Bank shall establish a regulatory compliant organic framework to protect the rights of its data subjects and preserve the confidentiality, integrity and availability of personal data, ensuring that the Bank's personal data processing systems are reasonably secured, protected, selectively accessible and processed or utilized for valid purposes only with internal measures on detecting and monitoring breaches and security incidents.

A. DATA PRIVACY GOVERNANCE

1. Oversight

The Bank's Board of Directors and Senior Management shall have overall oversight on the compliance with the Act and the implementation of this Policy and other related policies of the Bank.

The President and Chief Executive Officer, as Head of Agency, shall ensure the provision of the necessary support and allocation of essential resources to effectively and efficiently operationalize a data privacy framework within the Bank. Together with Senior Management, he shall exercise decision-making and authority regarding data privacy matters that may affect the Bank's strategic and tactical plans. This includes the mandatory designation of a Data Protection Officer who shall be accountable for ensuring compliance with the Act and other applicable laws and regulations relating to privacy and data protection.

The Compliance Management Group shall be responsible for incorporating compliance to the Act in the Bank's compliance program. The Head of the Compliance Management Group/Chief Compliance Officer shall directly supervise the Data Protection Officer.

2. Data Protection Officer

A Data Protection Officer (DPO), who shall be an organic employee of the Bank, shall be appointed to oversee compliance with the Act and other similar regulations.

The DPO shall have the following duties and responsibilities:

a. Ensure compliance with the Act and its IRR as well as this Policy and other related policies of the Bank;
b. Ensure the regular review (at least annually) of the privacy related policies, guidelines and procedures of the Bank;
c. Coordinate with the relevant officer/s of the Bank responsible for information security management for the effective implementation of the Bank's information security measures to ensure confidentiality, integrity and availability of personal data;
d. Organize data privacy awareness seminars;
e. Coordinate with the Bank's Data Breach Response Team in the management of security incidents related to data privacy;
f. Oversee and coordinate the conduct of Privacy Impact Assessments (PIA) to identify privacy risks of the Bank;
g. Develop and implement remediation plans for privacy and information security risks in coordination with the information security office and process owners;
h. Monitor compliance with the Bank's privacy standards for third party providers and other entities with access to personal data under the control of the Bank; and
i. Ensure compliance by the Bank with the reportorial, registration and other regulatory requirements of the Commission.

3. Associate Compliance Officers (ACO)[1]

The ACO of any unit of the Bank which processes personal data shall be the Compliance Officer for Privacy within his area of accountability and shall have the following duties and responsibilities:

a. Understand the Bank's compliance obligations under the Data Privacy Act and related regulations;
b. 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 Bank, by embedding such policies and guidelines in the day-to-day processes and procedures of the Bank's unit;
c. Ensure the conduct privacy impact assessments as may be needed;
d. Coordinate with the DPO and the information security office in the development of controls and mitigation plans to address identified privacy risks;
e. Ensure the implementation of risk controls and mitigation plans in the Bank's unit;
f. Promote a culture of privacy in the Bank's unit;
g. Ensure that all members of the Bank's unit have the capability to comply with the privacy and information security requirements as provided by law, regulations or internal Bank policies and guidelines; and
h. Report immediately to the DPO any personal data security incident or personal data breach in accordance with the Bank's incident response policy and procedure.

4. Personal Data Processor/Handler

[1] Per DBP Compliance Manual, the Associate Compliance Officer (ACO) is the head of Unit/Department/RMC/Branch in the Bank

Each employee that processes or handles personal data shall have the following duties and responsibilities:

a. Understand the Bank's compliance obligations under the Act and related regulations;
b. Understand and comply with privacy and information security policies and procedures in the processing of personal data;
c. Report immediately to his/her respective ACO any personal data security incident or personal data breach in accordance with the Bank's incident response policy and procedure;
d. Regularly implement controls and mitigation plans to address privacy risks; and
e. Regularly attend or undergo privacy trainings and other learning activities.

B. PROCESSING OF PERSONAL DATA

1. Data Processing System

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

a. Bank units, employees or third parties with functions relating to personal data processing;
b. The categories of and inventory of data subjects and the types of personal data being processed;
c. 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;
d. The purposes for processing including any intended future processing or data sharing; and
e. The recipients or intended recipients of personal data.

2. Data Collection

a. 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, customer and employee forms):
    (i) Description of personal data to be processed;
    (ii) Purpose/s of processing;
    (iii) Scope and method of processing;
    (iv) Parties to whom the personal data may be disclosed;
    (v) Contact details of the Bank or its Data Protection Officer (DPO);
    (vi) Retention period; and
    (vii) His rights as data subject.

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

b. 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.

3. 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. Data Quality

   Data quality must be ensured when processing personal data.

   a. Personal data must be accurate, relevant and up-to-date for the purposes for which it is to be used.
   b. Inaccurate or incomplete data must be corrected, supplemented, destroyed or restricted for its further processing.

5. Proportionality of Processing

   Processing must be adequate and not excessive and must be in relation to the purposes for which they are collected and processed.

6. 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 of legal claims, for legitimate business purposes or as provided for by law.

7. Data Sharing

   The disclosure or the transfer of personal data to a third party for further processing shall comply with the following conditions:
   a. The consent of the data subject on data sharing must be obtained even when the data is to be shared with the Bank's subsidiaries or affiliates; and
   b. Any data sharing arrangement must be covered by a data sharing agreement which shall provide, among others, the data privacy and security standards to be observed.

8. Outsourcing

The Bank 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:

a. Set appropriate privacy and security standards (organizational, physical and technical measures) to be complied by the contractors or service providers when processing personal data.
b. Take into account in the accreditation, hiring and performance evaluation processes, the capability of the contractors or service providers to meet the privacy and security standards set by the Bank.
c. Embed privacy requirements, security standards, data breach management protocol and the right of the Bank to audit compliance with the foregoing requirements in the agreements with contractors or service providers.
d. Conduct compliance audits where appropriate.

C. RIGHTS OF DATA SUBJECTS

The rights of a data subject as provided in the Act should be observed when processing personal data, which shall include the following:

1. Right to be informed

The data subject has the right to be informed on the following matters:

a. Whether his personal data shall be, are being or have been processed;
b. The type of personal data to be entered into the data processing system;
c. The purpose/s for the processing;
d. The scope and method of processing;
e. The parties to whom the personal data may be disclosed;
f. Methods utilized for automated access if allowed by the data subject;
g. Contact details of the Bank or its representative;
h. Period for which the personal data will be stored; and
i. Existence of their rights as data subject.

2. The right to object

The data subject has a right to object to the processing of his/her personal data which may cause him damage or distress, as well as to the processing for direct marketing, automated processing or profiling. The data subject's objection to any of these purposes shall be made in writing and duly received by the Bank.

3. Right to access

The data subject has the right to reasonable access, upon demand, to the following:

a. Sources from which the personal information were obtained;
b. Name and address of the recipients of the personal data;
c. Manner by which the personal data was processed;
d. Reasons for the disclosure of the personal data to the recipients;

e. Information on automated processes where the personal data will or likely to be made as the sole basis for any decision significantly affecting or that will affect the data subject;
f. Date when his personal data was last accessed or modified; and
g. Name, address and contact details of the Bank or its representative.

4. Right to rectification

The data subject has the right to dispute the inaccuracy or error in his/her personal data and have the Bank correct it immediately and accordingly, unless the request is vexatious or unreasonable.

5. Right to erasure or blocking

The data subject has the right to suspend, withdraw or order the blocking, removal or destruction of his personal data from the Bank'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.

6. Right to be indemnified

The 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.

7. Right to lodge a complaint

The data subject has the right to lodge a complaint before the Commission for any violation of his or her rights granted under the Act.

8. Right to data portability

The data subject shall have the right to obtain from the Bank 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 the transfer of such personal data in an electronic or structured format to be issued by the Commission.

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

D. REGISTRATION AND OTHER COMPLIANCE REQUIREMENTS

1. Registration of Data Processing System/s

In view of the sensitive nature of client and employee personal information in its custody, the Bank is required to register its personal data processing system/s with the Commission.

2. Notification of Automated Processing System

   The Bank shall notify the Commission if:
   a. It carries out automated data processing which becomes the Bank's sole basis for decision-making about a data subject; and
   b. The decision would significantly affect the data subject.

3. Annual Report

   A general summary of the security incidents and data breaches hereof shall be submitted to the Commission annually in accordance with its rules.

4. Data Privacy Awareness Trainings

   Once a year, a mandatory, Bank-wide training on privacy and data protection policies shall be conducted. A similar training shall be provided during all new-employee orientations.

II. CONTROLS

A. SECURITY MEASURES

As a Personal Information Controller (PIC), the Bank imposes reasonable and appropriate physical, technical and organizational security measures which must be implemented to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. The security measures shall:

1. Promote privacy and data protection awareness in the Bank through seminars, trainings and regular communication.
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.
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. Privacy impact assessments of the Bank's personal data processing systems shall be conducted to identify and provide an analysis of data privacy risks and propose measures intended to address them.
5. Appropriate information security measures shall be adopted. In this regard, information security management policies are deemed incorporated in this Policy.

B. BREACH AND SECURITY INCIDENTS

The Bank implements policies and procedures for the management of a personal data breach, including security incidents and shall:

1. As part of its information security management system, establish administrative, preventive and detective 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.
2. Establish and implement a security incident management policy, which shall include the following:
    a. 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.
    b. Implementation of an incident response procedure including the execution of corrective actions and controls to:
        (i) Contain or mitigate the negative effect of a security incident, data breach, complaint, non-compliance or misconduct;
        (ii) Restore integrity of the information and communications system; and
        (iii) Improve the prevention and detection of future incidents.
    c. The conduct of internal investigation to understand facts, circumstances, root cause and appropriate resolution.
    d. The procedure for contacting law enforcement authorities in case a possible criminal act was committed.
    e. Compliance with the notification and reporting requirements of the Commission in the event of occurrence of personal data breach or security incident.

C. COMPLIANCE TESTING AND AUDIT

The bank shall ensure that according to identified risk level, audit and testing activities are conducted annually to identify gaps in the Bank's data privacy framework vis-à-vis compliance obligations.

D. NON-COMPLIANCE SANCTIONS AND PENALTIES

Violation of this Policy, the Act and its IRR, will be dealt with in accordance with an established disciplinary action and appropriate responses for potential legal actions, including civil and criminal actions.