LBP INSURANCE BROKERAGE, INC.
(A LAND BANK Subsidiary)

CLASS D

POLICY ON DATA PRIVACY

A. RATIONALE

LBP (LAND BANK OF THE PHIL.) INSURANCE BROKERAGE, INC. (LIBI) respects the right to privacy of every individual as enshrined in our Constitution and in our laws and most especially with respect to personal data privacy rights. This is in pursuance to the right of an individual to be free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned.

To ensure that personal data and information being processed by LIBI are secured and protected in accordance with the data privacy principles of transparency, legitimate purpose, and proportionality, these guidelines are hereby issued in compliance with Republic Act No. 10173, otherwise known as the Data Privacy Act (DPA) of 2012, its Implementing Rules and Regulations (IRR), National Privacy Commission (NPC) Circulars and other applicable laws.

B. OBJECTIVES

The guidelines aim to:

1. provide generally accepted principles and standards for personal data protection; and

2. ensure that personal data in the LIBI's information and communications systems are secured and protected.

C. COVERAGE

These guidelines shall cover the policies and procedures to ensure privacy and protection of personal and sensitive personal information of the data subject provided to or gathered by the company, as well as, incident management in case of personal data breach.

Information processed to comply with Republic Act (RA) No. 9160 (Anti-Money Laundering Act) and other applicable laws shall not be covered by the guidelines.

All personnel of LIBI whether regular or contractual, must strictly comply with the terms and provisions thereof.

D. DEFINITION OF TERMS

TERMS	DEFINITION
Consent of the Data Subject	any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal, sensitive personal, or privileged information about and/or relating to him or her; it is evidenced by written, electronic or recorded means; it may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so
Data Sharing	the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or personal information processor (PIP). In the case of the latter, such disclosure or transfer must have been upon the instructions of the PIC concerned; it excludes outsourcing, disclosure or transfer of personal data by a PIC to a PIP
Data Sharing Agreement	a contract, joint issuance or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties
Data Subject	an individual whose personal, sensitive personal, or privileged information is processed
Information and Communications Systems	a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or 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
Personal Data	all types of personal information, including those pertaining to LIBI personnel
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
Personal Data Processing System	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

TERMS	DEFINITION
Personal Information	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 LIBI or when put together with other information would directly and certainly identify an individual
Personal Information Controller (PIC)	a natural or juridical person, or any other body that controls the processing of personal data, or instructs another to process personal data on its behalf
Personal Information Processor (PIP)	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
Privacy Impact Assessment (PIA)	process undertaken and used by a government agency to evaluate and manage privacy impacts
Privileged Information	any and all forms of data which under the Rules of Court of the Philippines and other pertinent laws constitute privileged communication
Processing	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, erasure or destruction of data; 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
Security Incident	an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data; includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

TERMS	DEFINITION
Sensitive Personal Information	Personal information: 1. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; 2. about an individual's health, education, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; 3. issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, (for employees only,) and 4. specifically established by an Executive Order (EO) or an act of Congress to be kept classified
Vulnerable Group	may include children, older people, mobility impaired, mental/cognitive function impaired, sensory impaired, individuals supported by health or local authorities, temporarily or permanently ill, individual cared for by relatives, homeless, pregnant women, minority language speakers, tourists, and travelling community

E. GENERAL GUIDELINES

LIBI shall designate a Data Protection Officer (DPO), subject to confirmation of the Board. The DPO shall be responsible for the LIBI's compliance with the DPA.

2. LIBI shall designate a Compliance Officer for Privacy (COP).The COP shall assist the DPO in ensuring compliance with the DPA, and escalate to PIC any suspected or potential occurrence of personal data loss to breach to PIC.

3. Collection and Processing of Personal Data

a. Consent of the data subject shall be required prior to the collection and processing of personal data. The consent shall be limited to the declared, specified and legitimate purpose and may be withdrawn by the data subject.

b. The data subject shall be provided with specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of personal data for profiling, or processing for direct marketing, and data sharing.

c. Only personal data that is necessary shall only collects basic contact information of clients and customers, such as their full name, address, email address, contact number, together with the insurance that they would like to cover such mortgage redemption ,easy home loan, personal accident and life , bonds, comprehensive car insurance etc. The account officer attending to customers will collect such information through accomplished application forms.

d. Processing shall be transparent, and allow the data subject sufficient information to know the nature and extent of processing.

e. Information provided to a data subject shall always be in clear and plain language to ensure that they are easy to understand and access.

f. Processed personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Inaccurate or incomplete data shall be rectified, revised, supplemented, destroyed, or restricted for further processing.

g. Processing of sensitive personal and privileged information shall be prohibited, except in any of the following cases:

1) Consent is given by the data subject, or by the parties to the exchange of privileged information, prior to processing;

2) The laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data; and

3) Processing is necessary to:

a) protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express consent prior to processing; and

b) achieve the lawful and non-commercial objectives.

h. The personal data processing systems of LIBI shall be registered with the National Privacy Commission.

4. Storage of and Access to Personal Data

a. Hardcopies of personal data being processed by LIBI shall be stored in secured room and access shall be restricted to personnel that are authorized.

b. An access control system that records when, where and by whom the data center or the personal data are accessed shall be implemented.

c. Access to personal data by independent contractors, consultants and service providers engaged by LIBI, shall be governed by strict procedures contained in formal contracts, which provisions must comply with the Data Privacy Act, its IRR, and all applicable issuances by the NPC

5. Retention and Disposal of Personal Data

a. Retention and disposal of personal data shall be in accordance with Records Disposal policy of LIBI consistent with the National Archives Act of 2007.

b. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

c. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, as allowed by the existing law, may be stored for longer periods, subject to implementation of the appropriate security measures to safeguard the rights and freedoms of the data subject.

d. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

6. Data Sharing

a. Data sharing shall be allowed when the data subject consents to the same. The following information shall be provided to the data subject before data sharing:

1) Identity of the PIP who has access to the personal data;

2) Purpose of data sharing;

3) Categories of personal data sharing;

4) Intended recipients or categories of recipients of the personal data;

5) Existence of the rights of data subjects, including the right to access and correction, and the right to object; and

6) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

b. Data sharing shall also be allowed when it is expressly authorized by law and processing adheres to the principles of transparency, legitimate purpose and proportionality.

c. Data sharing between LIBI and other parties for the purposes of public function or provision of a public service shall be covered by written data sharing agreement which shall comply with Section 6 of NPC Circular No. 16"02 ***(Annex A).***

d. The terms and conditions of a data sharing agreement shall be subject to a mandatory period review upon the expiration of its term, and any subsequent renewal or extensions thereof. The review shall include:

1) reasons for the termination, renewal and/or extension of the agreement; and

2)' in case of renewal, any changes made to the terms and conditions of the agreement.

e. Data Sharing Agreement may be terminated on the following grounds:

1) expiration of the term or any valid extension thereof;

2) agreement by the parties;

3) commission of breach by any of the parties;

4) in case of disagreement, if the NPC finds the continued existence of agreement is no longer necessary and/or is contrary to public interest or public policy.

f. All personal data transferred to other parties by virtue of data sharing agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement, unless otherwise provided by such agreement.

7. Sec rity Measures
u

a. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research. LIBI shall ensure appropriate privacy and security safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.

b. A reasonable and appropriate security measures for the protection of personal data shall be implemented by LIBI.

1) Organizational Security Measures

a) LIBI, through the DPO shall conduct PIA consistent and proportionate with the size and sensitivity of the personal data being processed including the risk of harm from the unauthorized processing of that data. The PIA shall be conducted before:

1} Initiating a privacy management program;

2} Implementing new business process or a new technology;

3} Scaling up an existing business process or usage of technology;

4} Entering to a data sharing agreement;

5} Implementing any type of large-scale data collection; and

6} Outsourcing any type of processing to service provider.

b) The PIA shall include the following:

1} data inventory

a} types of personal data;
b} repository holding personal data;
c} media used storing personal data; and
d} risks associated with the processing of the personal data

2} systematic description of the processing operations anticipated and the purpose of the processing, including, where applicable, the legitimate interest pursued by LIBI

3} assessment of the necessity and proportionality of the processing in relation to the purpose

4} assessment of the risks to the rights and freedoms of data subjects

c) LIBI shall sponsor a mandatory training on data privacy and security in its premises at least once a year. For PIP, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

d) All employees including third party service providers shall be required to sign either a Non-Disclosure Agreement, Confidentiality Agreement, or Data Sharing Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

2) Physical Security Measures

a) All personal data processed by LIBI shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by LIBI

b) LIBI shall enforce an access control system that records when, where, and by whom the data centers are accessed.

c) Transfer of personal data by email must be secured by passwords.

d) Transmittal of documents or media containing personal data by mail or post shall make use of registered mail or where appropriate, guaranteed parcel post service. It shall establish procedures that ensure that such documents or media are delivered only to the person to whom they are addressed, or his or her authorized representative.

3) Technical Security Measures

a) LIBI shall use an intrusion detection system to monitor security breaches and alert LIBI of any attempt to interrupt or disturb the system including our Endpoint Protection Standard/Policies.

b) LIBI shall review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

c) Implement access controls to prevent the PIP from printing or copying personal data to personal productivity software like word processors and spreadsheets that do not have any security or access controls in place.

d) Only known devices, properly configured to LIBI's security standards, are authorized to access personal data. It shall also put in place solutions, which only allow authorized media to be used on the computer equipment.

e) LIBI shall review security policies, conduct vulnerability assessments and perform penetration testing within LIBI's premises on regular schedule to be prescribed by the appropriate department or unit.

c. Any person involved in the processing of personal data shall maintain records and identify the duties and responsibilities of individuals who have access to personal data. Records shall include

1) information about the purpose of the processing, including any intended future processing or data sharing;

2) description of all categories of data subjects, personal data, and recipients of personal data that will be involved in the processing;

3) general information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;

4) general description of the organizational, physical, and technical security measures in place; and

5) name and contact details of the individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

8. Personal Data Breach Management

a. The Management thru a Special Order shall designate a Breach Response Team with the DPO as the Team Leader. The team shall be composed of representatives from various groups/units. The members of the Team shall be officer-level with authority to decide and shall be called upon only if the data breach concerns their group/units

b. The Breach Response Team shall be responsible for the documentation of all actions taken by LIBI relating to personal data breach. Reports shall include:

1) Description of the personal data breach, its root cause and circumstances regarding its discovery;

2) Actions and decisions of the incident response team;

3) Outcome of the breach management, and difficulties encountered; and

4) Compliance with notification requirements and assistance provided to affected data subjects.

c. It is the responsibility of the Breach Response Team to ensure that all security incidents on personal data breaches shall be documented through written reports, including those not covered by the notification requirements.

1) In the event of a personal data breach, a report shall include the facts surrounding the incident, the effects of such incident, and the remedial action taken by LIBI

2) Any or all reports shall be made available when requested by the NPC. A summary of all reports shall be presented to the Audit and Risk Com; to be elevated to the Board and submitted to the NPC annually by the DPO. The report shall comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

d. It shall be the responsibility of the DPO to come up with a comprehensive security incident management policy taking into account LIBI's various operations processing of personal data and the results of the PIA. Existing company policies that affect or tend to affect data protection shall be reviewed by Audit & Riskcom and accordingly amended, repealed or adopted, to come up with a comprehensive security incident management policy.

e. The security incident management policy shall include measures intended to prevent or minimize the occurrence of a personal data breach. Safeguards may include:

1) Regular conduct of PIA to identify attendant risks in the processing of personal data;

2) Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;

3) Regular monitoring for security breaches and vulnerability scanning of computer networks;

4) Capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents; and

5) Procedure for the regular review of policies and procedures, including the testing, assessment, and evaluation of the effectiveness of the security measures.

f. It shall also be the responsibility of the DPO to come up with a more detailed procedure in handling data breach incidents. The guidelines on breach notification shall be incorporated and harmonized with existing company procedures relating to handling of data breach incidents.

g. The Breach Response Team shall be responsible for LIBI's compliance with the notification requirements in case of personal data breach. The Breach Response Team shall secure clearance from the General Manager, Admin Head and the President and CEO to make the notification bearing in mind the periods set under the law and existing rules and issuances.

h. The DPO upon the recommendation of the Breach Response Team and approval of the appropriate authorities (Audit & Risk, Excom & Board) shall notify the NPC and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred, under the following conditions:

1) personal data involves sensitive personal information or any other information that may be used to enable identity fraud;

Note: Other information shall include, but not limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Phi/health, SSS, GS/S and TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

2) information may have been acquired by an unauthorized person; and

3) unauthorized acquisition will give rise to a real risk of serious harm to any affected data subject.

i. In case of uncertainty as to the need for notification, The Audit and Riskcom shall review and elevate to the Board, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The Breach Response Team shall include an evaluation if the personal data reasonably believed to have been compromised involves:

1) Information that would likely affect national security, public safety, public order, or public health;

2) At least 100 individuals;

3) Information required by applicable laws or rules to be confidential; or

4) Personal data of vulnerable groups.

j. The Breach Response Team shall observe the following in notifying the NPC:

1) The NPC shall be notified within 72 hours upon knowledge of or the reasonable belief after evaluation and assessment by Audit and Riskcom that a personal data breach has occurred.

2) Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. LIBI need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects.

3) There shall be no delay in the notification if the breach involves at least 100 data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the NPC shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days from the discovery of the breach unless LIBI is granted additional time by the NPC to comply. It shall be the responsibility of the Breach Response Team to request such extension.

4) The notification shall include, but not limited to:

a) nature of breach;
b) personal data possibly involved; and
c) measures taken to address the breach.

5) Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification. The report shall also include the name and contact details of the DPO. Where applicable, the manner of notification of the data subjects shall also be included in the report.

6) The DPO shall ensure that the NPC receives the report and that the LIBI receives the copy of confirmation of NPC if done electronically. A report is not deemed filed without such confirmation.

k. The Breach Response Team shall observe the following in notifying the data subjects:

1) The data subjects shall be notified within 72 hours upon knowledge of or reasonable belief by LIBI that a personal data breach has occurred. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

2) If it is not reasonably possible to notify the data subjects within the prescribed period, LIBI through the Breach Response Team, shall request the NPC for an exemption from the notification requirement, or the postponement of the notification.

3) The notification to the data subject shall include, but not limited to:

a) nature of the breach;

b) personal data possibly involved;

c) measures taken to address the breach;

d) measures taken to reduce the harm or negative consequences of the breach;

e) the name of the DPO or his representative, including his or her contact details from whom the data subject can obtain additional information regarding the breach; and

f) any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

l. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The Breach Response Team shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. Where individual notification is not possible or would require a disproportionate effort, LIBI through the Breach Response Team may seek the approval of the NPC to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner.

9. Inquiries and Complaints

a. Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the control and custody of LIBI, including the data privacy and security policies implemented to ensure the protection of their personal data. They may forward their inquiries/complaints to LIBI thru the Admin Head or DPO together with their contact details for reference.

b. LIBI shall take appropriate action on the claimed privacy violation or personal data breach within 15 days from receipt of the complaint.

F. DUTIES AND RESPONSIBILITIES

1. DPO shall:

a. Oversee the compliance of the organization with the DPA, its IRR, and other related polices, including issuances of the NPC;

b. Inform and cultivate awareness on personal data protection and privacy obligations within the company;

c. Act properly and in a timely manner, in all issues which relate to privacy and data protection;

d. Coordinate with those who are responsible for related functions within the organization;

e. Ensure the conduct of PIA, relative to activities, measures, projects, programs or systems of the Company;

f. Initiate the establishment and implementation of a privacy management program, including continuous assessment and revision;

g. Oversee the implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure;

h. Keep up-to-date on relevant privacy issues and appropriate data protection practices;

i. Maintain confidentiality concerning the performance of assigned tasks;

J. Advise the Audit & Risk Com then elevate to the Board regarding

complaints and exercise by data subjects of their rights;

k. Advocate for the development, review and revision of policies, guidelines, projects and programs of the Company relating to privacy and data protection by adopting a privacy by design approach;

l. Serve as the contact person of LIBI vis-a-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the organization; and

m. Report data breach to the NPC.

2. COP shall:

a. Assist the DPO in the performance of his/her functions; and

b. Escalate any suspected or potential occurrence of personal data breach to Breach Response Team for evaluation/assessment.

3. Breach Response Team shall:

a. Implement the security incident management policy of LIBI;

b. Manage security incidents and personal data breaches, including assessing and evaluating of security incidents, restoring integrity to the information and communications system, mitigating and providing remedy to any resulting damage;

c. Recommend to the Board of Directors through Audit & Riskcom appropriate actions pertaining to data breach notification procedure and other processes relating thereto;

d. Comply with documentation and reporting requirements required by the DPA, its IRR and related issuances by the NPC on personal data breach management; and

e. Comply with the relevant provisions of the DPA, its IRR, and all related issuances by the NPC on personal data breach management.

. LIBI thru the Audit & Risk Com shall:

a. Effectively communicate to all personnel the designation of the DPO and COPs, including their functions;

b. Allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;

c. Provide sufficient time and resources for the DPO to keep updated with the developments in data privacy and security and to carry out the tasks;

d. Grant the DPO appropriate access to the personal data the company is processing, including the processing systems;

e. Coordinate with the DPO in the event of a personal data breach or security incident; and

f. Ensure that the DPO is made part of all relevant working groups that deal with personal data processing activities.

Note: The Company shall not directly or indirectly penalize or dismiss the DPO for non performance his/her tasks.

G. PENALTIES/SANCTIONS

1. A penalty of imprisonment and fine shall be imposed on any person who perform processing of, provide access to, or dispose of personal information and sensitive personal information without the consent of the data subject, or without being authorized under any existing law as shown in the table below:

Punishable Act of LIBI Employees	Personal Information		Sensitive Personal Information	
	Jail Term	Fine (in P)	Jail Term	Fine (in P)
Unauthorized Processing *(Section 25)* Processing of personal or sensitive personal information without authorization or consent of the data subject	1 to 3 years	500kto 2M	3 to 6 years	500kto 4M
Accessing . of Information Due to Negligence *(Section* 26) Providing access to personal or sensitive personal information, due to negligence, without authorization :	1 to 3 years	500kto 2M	3 to 6 years	500kto 4M

CLASS D

Punishable Act of LIBI Employees	Personal Information		Sensitive Personal Information	
	Jail Term	Fine (in P)	Jail Term	Fine (in P)
Improper Disposal *(Section* 27) Knowingly or negligently disposing, discarding, or abandoning personal or sensitive personal information in an area accessible to the public or	6 months to 2 years	100k to 500k	1 to 3 years	100kto 1M
Processing of Information for Unauthorized Purposes (Section 28) Processing of personal or sensitive persona information for purposes not authorized by the data subject	18 months to 5 years	500kto 1M	2 to 7 years	500kto 2M
Unauthorized Access or Intentional Breach (Section 29) Knowingly and unlawfully, or violating data confidentiality and security data systems breaking in in any way into any system where personal or sensitive persona information are stored	1 to 3 years	500kto 2M	1 to 3 years	500kto 2M
Concealment of Security Breaches *(Section* 30) Intentionally or by omission concealing the fac of occurrence of security breach, after having knowledge of the incident and of the obligation to notify NPC pursuant to Section 20(f) of the DPA	18 months to 5 years	500kto 1M	18 months to 5 years	500kto 1M
Malicious Disclosure *(Section* 31) Disclosing unwarranted or false information relative to any personal or sensitive persona information obtained in bad faith or with malice	18 months to 5 years	500kto 1M	18 months to 5 years	500kto 1M
Unauthorized Disclosure *(Section* 32) Disclosing personal or sensitive persona information to a third party, not covered in the preceding punishable act without the consent of the data subject	1 to 3 years	500kto 1M	3 to 5 years	500kto 2M

Punishable Act of LIBI Employees	Personal Information		Sensitive Personal Information	
	Jail Term	Fine (in P)	Jail Term	Fine (in P)
Combination or Series of Acts *(Section* 33) Any combination or series of punishable acts as defined above	3 to 6 years	1M to 5M	3 to 6 years	1M to 5M

Any violation on the DPA shall be subject to the provisions of the Revised Penal Code, the LIBI's policies and guidelines on administrative and disciplinary cases, and other relevant laws and regulations.

2. Violations of rules on data sharing shall be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fine. Failure to comply may be ground for administrative and disciplinary sanctions against any erring employee in accordance with existing laws and regulations.

H. INTERNAL CONTROLS

1. A training on privacy and data protection policies shall be conducted annually. Same shall also be included during personnel orientations to all personnel including members of the Audit & Riskcom

2. All personnel concerned shall strictly observe issuances related to information security and handling data.

3. LIBI shall conduct regular review and revision , at least annually, of policies and procedures. The DPO shall ensure the regular conduct of assessment and evaluation of the effectiveness of the security measures.

4. Retention and disposal of records/documents shall be in accordance with LIBI's approved Records Disposition Schedule.

I. TRANSITORY PROVISION

1. All IT systems which are digitally processing personal data shall be reviewed to determine compliance to the mandated encryption requirements.

2. Assessment shall be conducted if there are technologies that will prevent files with personal data from being copied to local machine or if there are existing IT infrastructure controls and measures that can be utilized to achieve the same purpose.

3. All existing data sharing agreements shall be reviewed by the concerned parties to determine the compliance with the DPA, its IRR, issuances by the NPC and other laws and regulations.

4. An existing data sharing agreement found to be compliant except for the requirements regarding consent shall be allowed to continue until the expiration of such agreement or until October 2018, whichever is earlier.

5. If an existing data sharing agreement is not for the purpose of performing a public function or providing a public service, the parties thereto shall immediately terminate the sharing or transfer of personal data. Any or all related contracts predicated on the existence of such agreement shall likewise be terminated for being contrary to law.

J. EFFECTIVITY

This Order shall take effect upon approval.

TOMAS T. DE LEON, JR.
PRESIDENT