Privacy Management Program

MANILA BANKERS
LIFE INSURANCE CORPORATION

Foreword

Gentlemen:
In the digital age, we offer our customers the freedom and convenience to transact online. This requires data to be collected and processed. When processing, storing and transmitting data, we must ensure a high level of data protection and data security. This standard must be in place for all the subjects we deal whether they be our brokers/agents, employees, clients, or industry partners.

For this purpose, we must set the standard in data protection. It is our duty as a member of the insurance industry to comply with Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012, the rules and regulations of the National Privacy Commission because protecting the personal rights and privacy of each data subject has become the foundation of trust in our business relationships.

Our Corporate Privacy Management Program lays out strict requirements for processing personal data pertaining to customers, prospects, business partners and employees. It meets the standards set forth in the Data Privacy Act. The policy sets applicable data protection and security standard for our company and regulates the sharing of information between our group companies. We have established data protection policies – transparency, legitimacy, and proportionality.

Our managers and employees are obligated to adhere to the Corporate Data Protection Policy and observe the data protection laws. As the Data Protection Officer, it is my duty to ensure that the rules and principles of data protection at Manila Bankers are followed with a high sense of accountability.

I will be pleased to answer any questions you have about data protection and security at Manila Bankers.

Gabriela E. Calma-Chan
Data Protection Officer

Contents

I.
Mission and Vision Statement

PRIVACY MISSION

The Manila Bankers Life Insurance Corporation works to protect the privacy of each and every individual who shares their personal data with us through strict adherence to the relevant laws, rules and regulations published by the National Privacy Commission, taking into account industry best practices. By establishing a culture of privacy and accountability among our staff and partners, we ensure the proper use and disclosure of all confidential and personal information. It is our mission to develop an environment that encourages the free flow of information while respecting the right of each individual to privacy.

It is the thrust of Manila Bankers Life Insurance Corporation to provide its clients and partners a digital environment which they can trust completely, that adheres to all relevant laws on privacy including the Data Privacy Act of 2012 and issuances of the National Privacy Commission. We greatly value the trust reposed to us, not just by our clients, but especially our partners and agents. Hence, in order to care for this trust, we take all steps necessary to safeguard all the information that is shared to us and we are committed to protect the confidentiality, integrity, and availability of these information with the view to create and maintain a safe digital space for those who conduct business with us.

VISION STATEMENT

Manila Bankers Life Insurance Corporation began in 1967 and has continued to be one of the long-standing life insurance corporations in the Philippines to date. It boasts of a national heritage, having been established by former legislator Senator Gil Puyat, Jr. As we take Manila Bankers Life Insurance Corporation to the age of digital technology, and the age of continuous _____, we firmly adhere to all relevant laws on data privacy. Conducting business in this digital age has set a new landscape where privacy is the new proxy for trust. Bearing this in mind, we take Manila Bankers Life Insurance Corporation to the digital age, with the ease of doing business and a reputation synonymous to privacy.

II.
Aim of the Data Protection Policy

Manila Bankers Life Insurance Corporation (Manila Bankers) is committed to compliance with the data protection laws. The Data Protection Policy applies across all related companies and is based on globally accepted, basic principles on data protection. In the digital age, privacy has become the proxy of trust, and data protection is the foundation of trustworthy business relationships.

The Data Protection Policy ensures and provides the adequate level of data protection prescribed by the National Privacy Commission and the national laws for cross-border data transmission.

III.
Scope and amendment of the Data Protection Policy

This Data Protection Policy applies to all related companies of Manila Bankers, i.e. IMG, Kaiser and its dependent group companies, affiliated companies, and their employees. For this purpose, "Dependent" means that Manila Bankers may enforce the adoption of this Data Protection Policy directly or indirectly, on the basis of majority management representation or by agreement. The Data Protection Policy extends to all processing of personal data. However, to be clear, anonymized data, e.g. for statistical evaluation or studies, is not subject to this Data Protection Policy.

Affiliates and related companies are not entitled to adopt regulations that deviate from this Data Protection Policy. Additional data protection policies can be created in agreement with the Data Protection Officer. This Data Protection Policy can be amended in coordination with the appointed Data Protection Officers under the defined procedure for amending policies. The amendments will be reported immediately to the Chief Executive Officer of Manila Bankers using the process for amending policies. Amendments that have a major impact on compliance with the Data Protection Policy must be reported annually to the data protection authorities that issue approval for this Data Protection Policy as Binding Corporate Rules.

The latest version of the Data Protection Policy can be accessed with the data privacy information at Manila Bankers website at: www.manilabankerslife.com

IV.
Application of national laws

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

Each company is responsible for compliance with this Data Protection Policy and the corresponding legal obligations. If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the relevant company must inform the Data Protection Officer. In the event of conflicts between national legislation and the Data Protection Policy, Manila Bankers will work with the relevant company to find a practical solution that meets the purpose of the Data Protection Policy.

V.
Principles for processing personal data

The Data Privacy Act of 2012 has laid down the three main principles for processing of personal data. These main principles are transparency, legitimate purpose, and proportionality. Adherence to these principles are required in the collection, processing, and disclosure of information.

1. FAIRNESS AND LAWFULNESS

When processing personal data, the individual rights of the data subjects must always be protected. The purpose of collection must be for legitimate purposes. Personal data must be collected and processed fairly and lawfully at all times.

2. RESTRICTION TO A SPECIFIC PURPOSE

Personal data can be processed only for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection and subsequently processed in a manner that is consistent with specified and legitimate purposes.

3. TRANSPARENCY

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- The identity of the Personal Information Controller
- The purpose of data processing
- Third parties or categories of third parties to whom the data shall be transmitted
- The rights of the Data Subject and how they may be exercised
- Security of Information
- Information how the data is stored and the period of retention
- Changes and updates to the privacy policy

4. DATA REDUCTION AND DATA ECONOMY

When we speak of proportionality there is reference to data reduction and data economy. Before processing personal data, one must determine to what extent the processing of personal data is necessary in order to achieve the purpose for which it is collected. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law. In sum, collection must be adequate and not excessive.

5. DELETION

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. FACTUAL ACCURACY; UP-TO-DATENESS OF DATA

Personal data on file must be accurate, relevant, complete, and when necessary for the purpose collected and processed, kept up to date. Data that is inaccurate or incomplete must be corrected, supplemented, destroyed, or in special cases, restricted from further processing.

7. CONFIDENTIALITY AND DATA SECURITY

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational, physical, and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

VI.
Reliability of data processing

Collecting, processing, and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

1. CUSTOMER AND PARTNER DATA

1.1 Data processing for a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

1.2 Data processing for advertising/ marketing purposes

If the data subject contacts Manila Bankers to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted.

Customer loyalty or advertising/marketing measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. Furthermore, the data subject must be informed about the use of his/her data for advertising/marketing purposes.

The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone. Refer to Figure 1 for Sample Consent Form.

If the data subject refuses the use of his/her data for advertising/marketing purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

1.3 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with IV.3. of this Data Protection Policy. Refer to Figure 2 for the Privacy Notice.

The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. For the protection all parties concerned, the granting of consent must be documented.

1.4 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

1.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for legitimate interests of Manila Bankers. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for purposes of legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

1.6 Processing of highly sensitive data

Highly sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

1.7 Automated individual decisions

Automated processing of personal data that is used to evaluate certain aspects (e.g. insurability) cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

1.8 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, provided information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy notice. Personal tracking may only be effected if it is permitted upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy notice.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

If files or documents are transmitted through the internet and made accessible to registered users, in addition to the requirement of identification and authentication of the recipient, the files or documents must be encrypted based on standards provided for by the NPC.

2. EMPLOYEE DATA

2.1 Data processing for the employment relationship

In employment relationships, personal data can be processed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other related companies.

In existing employment relationships, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

2.2 Data processing pursuant to legal authorization

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions under DPA of 2012. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national data protection legislation.

2.4 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with IV.3. of this Data Protection Policy. The DPA of 2012 defines consent of the data subject as, "freely given, specific, informed, indication of will" Furthermore, consent of the employees are not to be presumed by the mere fact that their employment has been engaged by Manila Bankers.
(See FIGURES 3 and 4)

FIGURE 3: DOCUMENTATION ON TRANSFER OF PD

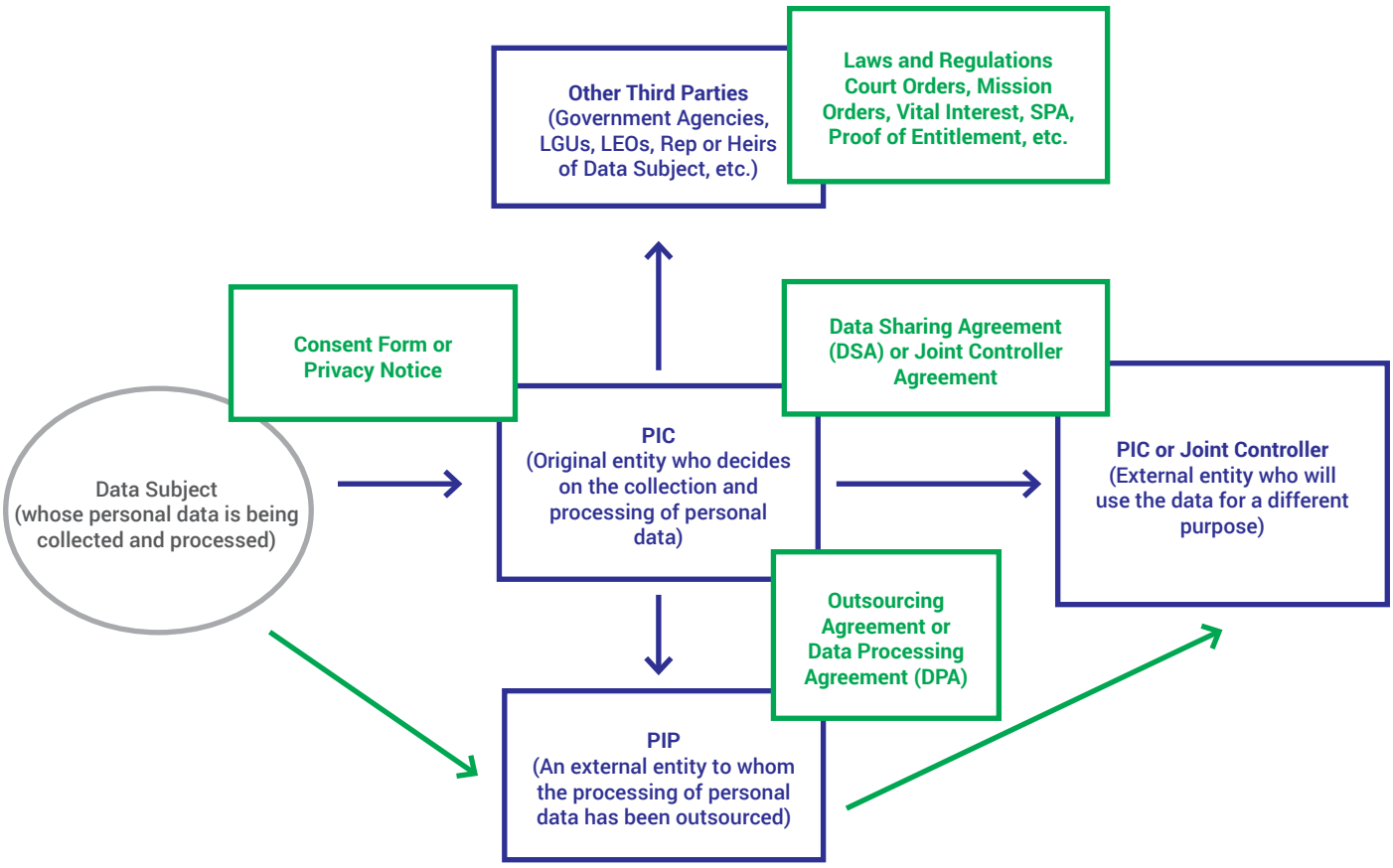


FIGURE 4: BASIS FOR PROCESSING

Basis	For PI	For SPI
Consent of Data Subject	Prior to collection or as soon as practicable and reasonable	Prior to processing
Contractual Agreement	To take steps at the request of the DS prior	
Legal Obligation	Compliance by PIC	Existing laws and guarantees protection of personal data
To protect vital interests	Vital interest of DS including life and health	AND the DS is not able to express consent
For medical treatment		Medical practitioner/institution and adequate level of protection of SPI
Lawful and Noncommercial Objectives		Confined to members of the organization and not shared
Public Order & Safety	To respond to national emergencies or public order and safety	
Legitimate Interests of PIC	Except where interests are overridden by rights and freedoms	
Public Authority	Constitutional/Statutory mandate	For the protection of lawful rights and interests of persons in proceedings
N/A	Criminal/administrative/tax liabilities	

2.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of Manila Bankers. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under the law (e.g. rights of the data subjects) must be taken into account.

2.6 Processing of highly sensitive data

Highly sensitive personal data, also referred to as Sensitive Personal Information, can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, marital status, and the health and sexual life of the data subject, information peculiar to an individual as assigned by government agencies, and information specifically established by law to be kept classified . Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under relevant laws. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfill its rights and duties in the area of employment law. The employee can also expressly consent to processing.
If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

2.7 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.8 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed where applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the company's network that block technically harmful content or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of the Manila Bankers. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant laws must be observed in the same manner as company regulations.

VII.
Transmission of personal data

Transmission of personal data to recipients outside or inside Manila Bankers is subject to the authorization requirements for processing personal data under V. The data recipient must be required to use the data only for defined purposes.

In the event that data is transmitted to a recipient outside Manila Bankers' to a third country, this country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation. A legal obligation of this kind can be based on the laws of the domiciliary country of the company transmitting the data. In the alternative, the laws of the domiciliary country of the company can acknowledge the purpose of data transmission based on the legal obligation of a third country.

If data is transmitted by a third party to a company, it must be ensured that the data shall be used for the intended purpose.
(See Figure 9)

VIII.
Contract data processing

Data processing through Personal Information Processors (PIP) means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing by PIP must be concluded with external providers and among companies within Manila Bankers. The client retains full responsibility for correct performance of data processing. The provider can process personal data only based on the instructions from the client. When issuing the order, the following requirements must be complied with the department placing the order must ensure that they are met.

1. The provider must be chosen based on its ability to cover the required organizational, technical, and physical protective measures.

2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.

3. The contractual standards for data protection provided by the Data Protection Officer must be considered.

4. Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

5. In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. By way of example, personal data from the European Union can be processed in a third country only if the provider can prove that it has a data protection standard equivalent to this Data Protection Policy. Suitable tools can be:
   a. Agreement on EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors.

   b. Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

   c. Acknowledgment of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

(See Figure 5, 6 and 7)

IX.
Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject. See Policies for the procedure for the exercise of the Rights of the Data Subject.

1. RIGHT TO BE INFORMED.

The data subject has the right to be informed if personal information pertaining to him/her shall be, are being, or have been processed. The data subject must be furnished information before entry into the processing system or at the next practical opportunity. When processing sensitive personal information, the data subject must always before informed prior to processing. Furthermore, when processing data, the data subject must be furnished information regarding the following (See FIGURE 2):

1. A description of the personal information to be processed
2. The purpose of processing
3. The scope and method of the processing
4. The recipients or categories of recipients to whom they may be disclosed
5. The methods of processing employed
6. The identity and contact details of the Personal Information Controller (PIC)
7. The period of retention
8. The existence of the data subject's rights

2. RIGHT TO ACCESS.

The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose, whether personal data was disclosed to third parties and the reasons therefore, the date when the data was last accessed or modified, and the designation and identity of the PIC. For employer/employee relationship, if there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain. If personal data is transmitted to third parties, information must be given about the identity of the third party to whom data is disclosed

3. RIGHT TO CORRECT.

If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

4. RIGHT TO OBJECT.

The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.

5. RIGHT TO BLOCK/REMOVE.

The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

6. RIGHT TO DATA PORTABILITY.

When personal information is stored in an electronic format, the data subject has the right to request for a copy of the personal information pertaining to him from the PIC, and when so requested, the PIC must oblige.

7. RIGHT TO FILE A COMPLAINT.

In cases where the data subject suspects a violation of his rights under the relevant laws, s/he may file a complaint directly with the PIC or with the National Privacy Commission as the case may be.

8. RIGHT TO BE INDEMNIFIED.

The data subject has the right to be indemnified for damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.
(See Policies on the Exercise of the Rights of the Data Subject)

X.
Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.
(See Policies on Security Clearances)

XI.
Processing security

Personal data must be protected from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical, physical, and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art technology, the risks of processing, and the need to protect the data (determined by the process for information classification).

In particular, the responsible department can consult with its Information Technology Officer (ITO) and Compliance Officer. The technical, physical, and organizational measures for protecting personal data are part of Corporate Information Security Management and must be adjusted continuously to the technical developments and organizational changes.

XII.
Data protection control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer in coordination with departments heads, Compliance Officers for Privacy, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Data Protection Officer. The Board of Manila Bankers must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under the law.

XIII.
Data protection incidents

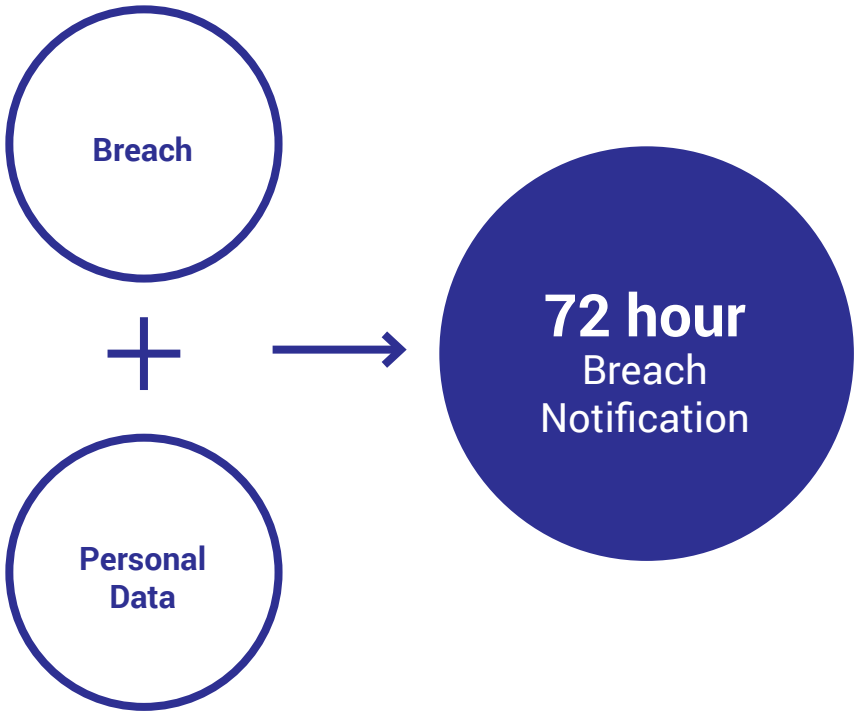
All employees must inform their supervisor, data protection coordinator or the Data Protection Officer immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or the unit is required to inform the responsible data protection coordinator or the Data Protection Officer immediately about data protection incidents.

In cases of

- improper transmission of personal information to unauthorized third parties, likely to cause danger or harm to the concerned data subject
- improper access by unauthorized third parties to personal data, or
- loss of personal data

the required company reports must be made immediately and without delay to the Data Protection Officer so that any reporting duties under the law can be complied with.
(See Figure 8)

FIGURE 8: SECURITY INCIDENTS



XIV. Responsibilities and Sanctions

The executive bodies of the Group companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met (e.g. national reporting duties). Management staff are responsible for ensuring that organizational, human resources, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the Data Protection Officer must be informed immediately. (See data breach response team)

The relevant executive bodies must inform the Data Protection Officer as to the name of their data protection coordinator. Organizationally speaking, in agreement with the Data Protection Officer, this task can be performed by a Compliance Officer for Privacy for multiple companies. Compliance Officer for Privacy are the contact persons on site for data protection. They can perform checks and must familiarize the employees with the content of the data protection policies. The departments responsible for business processes and projects must inform the Deputy Compliance Office within a reasonable time about new processing of personal data for the conduct of Privacy Impact Assessments (See Policies for the Conduct of Privacy Impact Assessments). For data processing departments that may pose special risks to the individual rights of the data subjects, the Data Protection must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers must ensure that their employees are sufficiently trained in data protection. You may coordinate with the Data Protection Officer for the conduct of Privacy Training and updates.

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted and may result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under the labor law.

XV.
Data Protection Officer

The Office of Data Protection shall be autonomous and the Data Protection Officer shall be internally independent of professional orders, works towards the compliance with national and international data protection regulations. S/he is responsible for the Data Protection Policy, and supervises its compliance. The Data Protection Officer is appointed by the Board of Directors of Manila Bankers and must be registered with the National Privacy Commission.

The Data Protection Officers of affiliate companies, together with the Deputy Compliance Officer shall work together and shall promptly cascade information on any data protection risks.

Any data subject may approach the Data Protection Officer, or the relevant or immediate department head of Manila Bankers for proper cascading to the Office of Data Protection, at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

If the immediate department head in question cannot resolve a complaint or remedy a breach of the Policy for data protection, the Data Protection Officer must be consulted immediately. Decisions made by the Data Protection Officer to remedy data protection breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must always be reported to the Data Protection Officer.

Contact details for the Data Protection Officer are as follows:

Data Protection Officer
9th Floor, King's Court Building 1, Don Chino Roces Avenue, Makati City
E-mail: dpo@manilabankerslife.com

XVI.
Definitions

- Act refers to Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012
- Commission refers to the National Privacy Commission
- Data is anonymized if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labor.
- 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/her personal, sensitive personal, privileged information. It may be also given on behalf of a data subject by a lawful representative or an agency specifically authorized by the data subject.
- Security Incident is an 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. This can pertain to actions by third parties or employees.
- Personal Data Breach refer to 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;
- Data subject under this Data Protection Policy is any natural person whose personal, sensitive personal information, and privileged information can be processed.
- Data Center or Data Room is a facility housing electronic (data center) or physical (data room) used for data processing, data storage, and for data center, communications networking. It is a centralized repository which may be physical or virtual used for the storage, management, and dissemination od data including personal data.
- Personal data refers to all types of personal information
- Personal Information refers to any information, in whatever form recorded, 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;

- Highly sensitive data or sensitive personal information is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Data relating to an individual's health, education, genetic or sexual life of a person, or to any 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. Data 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 denials thereof, suspension or revocation, and tax returns. Data specifically established by an executive order or an act of congress to be kept classified.

- Privileged Information refers to any and all forms of data which, under pertinent laws constitute privileged information.

- Processing personal data refers to any operation or any set of operations performed on personal data including the collection, recording, organization, storage, updating, or modification, retrieval, consultation, use, consolidation, blocking, 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.

- Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.

- Personal Information Controller is the legally independent company of the Manila Bankers, whose business activity initiates and dictates the relevant processing measure.

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

- Transmission is all disclosure of protected data by the responsible entity to third parties.

XVII.
Policies

All employees, agents, authorized representatives, and partners (collectively referred to as "Members") are covered by the Policies stated below. The Policies herein are crafted to meet the rights and obligations to all the members of MBLife and specifically adapted not only to comply with the requirements of the Data Privacy Act but to implement measures to ensure and protect the rights of each data subject that deals with MBLife in one way or another, whether they may be applicants, employees, or clients. The Policies shall be effective immediately.

POLICY FOR EXERCISE OF RIGHTS OF DATA SUBJECT

The data subjects may exercise their rights by filing a written request with the concerned member of MBLife with whom they are directly dealing with. Employees, as data subjects, may also exercise their rights by filing a written request with the HR Department. The procedure and the periods for exercising their rights can be found in the Data Security Manual Section II Processing of Personal Data under Use.

All requests of the data subject shall be immediately forwarded to the DPO who shall have 5 days to evaluate the request and decide whether or not to grant or deny the request. The requests must comply with the required information as provided in the Data Security Manual. The DPO shall have 30 calendar days from referral of the request to the DPO and submission of complete documents to comply unless a longer period is required.

When the request of the Data Subject shall require the production of a document or such other output, MBLife shall have the right to charge a reasonable fee, which shall be made known to the data subject prior to processing the request. If the DPO should deny the request, the DPO shall provide a written notice to the data subject denying the request and the reasons supporting the denial.

All affected employees shall comply with this Policy. Failure by any member of MBLife to comply with the foregoing shall be meted out with a penalty from Written Warning to Dismissal.

POLICY FOR SECURITY CLEARANCES

All department heads of MBLife shall immediately identify personnel handling personal data and provide their names and such other information to the DPO and the IT Department. The DPO shall keep a record of the personnel handling personal information, their contact details, and a description of the personal data they handle.

The IT Department shall ensure that prior to accessing personal information, the subject personnel shall be given a unique access code which shall identify the personnel when he/she is logging in the system to access or process personal data. Members handling personal data keep their unique access codes confidential. Disclosure of access codes is an offense which shall merit a penalty from Suspension to Dismissal.

Unless otherwise specified, violations under this Policy shall merit a penalty from Written Warning to Dismissal.

Lead
Department Heads handling Personal Data
IT Department Head

POLICY FOR CONDUCT OF PRIVACY IMPACT ASSESSMENT (PIA)

All departments who process personal data must register their program, project, process, measure, system, technology (PPPMST) with the DPO and conduct a Privacy Impact Assessment. The results of the PIA shall be completed not later than 30 days from the effectivity of the manual and the results, including the Personal Data Inventory (PDI), shall be made available to the DPO. After the initial conduct of the PIA, all department heads are required to conduct a PIA within 15days after every security incident or amendments to the PPMST or every year, whichever is sooner.

A copy of the format of the PIA can be found under FIGURE 11. Any questions with regard to the conduct of the PIA or any request for assistance to conduct the PIA shall be made by emailing the DPO with subject Privacy Impact Assessment. The DPO shall exert best efforts to conduct a PIA with the concerned department within 5 business days from request.

The conduct of PIA shall ensure that all the essential elements are met-

- Ownership of the PPPMST
- Stakeholder Involvement
- Privacy Risk Map
- Implementing Controls
- Management Approval
- Implementation and Monitoring Plan
- Review and Audit

The Department Heads shall be responsible for complying with this policy and failure to comply shall merit a penalty from Final Warning to Dismissal.

POLICY FOR PRIVACY NOTICES

All departments who collect personal data are required to secure consent consistent with the Data Protection Policies. In line with this, all departments, including branches of MBLife, are required to post in conspicuous places the Privacy Notice of MBLife so that all who deal with MBLIfe are properly appraised of our data protection policies. This shall also apply to all forms that require personal data to be filled up by the data subject. A copy of the Privacy Notice of MBLIfe can be accessed through the website. You may also secure a copy through the Data Protection Officer or request for a customized Privacy Notice to meet specific concerns of your data subjects by emailing dpo@manilabankerslife.com with the subject: Request for Privacy Notice.

The Privacy Notice shall be amended at least once every year on or before November 30 and shall contain the following information-

- What personal data is collected
- Who is collecting the personal data and how they may be contacted
- Why the data are being collected
- How long the data will be kept
- The fact that the data subject has rights relative to his/her personal data
- How such rights may be exercised
- How to contact the DPO
- How the privacy notice will be amended
- Failure to comply with this Policy shall merit a penalty from Written Warning to Dismissal.

POLICY FOR DO NOT CALL (DNC) LIST

For telemarketing, it is important to secure the consent of each data subject prior or reasonably after collecting personal information. Should the data subject refuse to give consent, the agent or employee of MBLife must take note of the request of the data subject and refer his/her contact details to the IT department who shall thereafter include the name and contact details of the concerned data subject to the DNC List. It is the responsibility of the IT Lead to ensure that those names under the DNC List shall not be contacted again.

Failure to comply with this policy shall merit a penalty from Final Warning to Dismissal.

Lead
Telemarketing Department
IT Department

POLICY FOR PASSWORDS AND SECURITY CODES

All computers and devices that are brought into the premises of MBLife shall be equipped with a password and security code. For personal devices, it is the responsibility of the user to equip the device with a password. For office-issued computers and devices, the IT Department, shall, upon issuing the device, provide a username and default password which shall be unique to the user and confidential. It is the responsibility of the user to immediately change the default password of the device. All passwords and security codes or access codes are strictly confidential and disclosure to third parties is strictly prohibited and punishable under this policy.

A violation of this policy shall merit a penalty from Written Warning to Dismissal.

POLICY FOR PRIVACY BY DESIGN (PBD)

Prior to the implementation of any Program, Process, Project, Measure, System, or Technology (PPPMST), a Privacy By Design must first be conducted. In PbD, privacy is the default setting and is incorporated into the PPPMST and customized towards data protection. Hence, all department heads who are looking to implement a new PPPMST must coordinate with the DPO to conduct a PbD, ensuring that the following are complied with PRIOR to the launch of the PPPMST-

- Impact Assessment
- Limit Data Collection
- Data Minimization
- Record Keeing
- Limit Processing
- Continuous Assessment

It is the responsibility of the process owner to ensure that PbD is conducted before implementation. A violation of this policy shall be punished from Written Warning to Dismissal.

POLICY FOR ACCESS PROCEDURES

Those requesting for access to the data center or data room must comply with the procedures set forth in the Data Security Manual on Access.

Within 30 days from the effectivity of this Data Protection Manual and the Data Security Manual, the IT Department and the Admin Department, in coordination with the DPO, shall meet and discuss-

- Security technologies that are virtualization-aware or enabled with security working at the network level rather than the server
- How to monitor everything continuously at the network level to be able to look at all assets (physical and virtual) that rest on the local area network, including those offline, and all inter-connections between them
- Acquisition of integrated families of products with centralized management that are integrated with or aware of the network infrastructure, or common monitoring capabilities for unified management of risk, policy controls, and network security
- Future and current needs and objectives at the design stage such as whether access to public cloud environments are required
- Policies and profiles that can be segmented and monitored in multi-tenant environments
-
- Create backups and redundancies to ensure business continuity and development

A violation of this policy shall be punished from Written Warning to Dismissal. If the a breach should occur due to non compliance with access procedures, then the maximum penalty shall be Dismissal.

Lead
IT Department
Admin Department

POLICY FOR SECURITY MEASURE IN COMPUTER SYSTEMS/ENCRYPTION

The IT Department shall ensure security measures are in place for computer systems, offline and online, including off-site access. For this purpose, the IT Department shall-

- Secure user authentication protocols
- Implement access control measures that restrict access to records and files containing personal data to authorized personnel and assigning unique identification and passwords to each person with computer access reasonably designed to maintain the integrity of the security of the access controls
- Encrypt all transmitted records and files containing personal data
- Provide reasonable monitoring of systems for unauthorized use of or access
- Encryption of all personal information stored on laptops and other portable devices
- Establish firewall protection and operating system security patches reasonably designed to maintain the integrity of the personal information
- Provide updated versions of system security agent software which must include malware protection, patches, and virus definitions
- Educate and train employees on the proper use of computer security system

For this purpose and in keeping with the standards set forth by the NPC, all personal data digitally processed must be encrypted whether at rest or in transit. MBLife shall comply with the recommended Advanced Encryption Standard with a key size of 256 bits (AES-256).

POLICY FOR PROPER DISPOSAL

All members of MBLife are required to properly dispose of all documents, physical or digital, containing personal data. For this purpose, papers or other physical document containing personal data shall not be used as scratch papers or otherwise reused. When no longer necessary, papers or other effects containing personal data must be completely shredded.

Electronic documents containing personal data must likewise be completely deleted, including deletion in the recycle bin, when no longer necessary. Furthermore, personnel of MBLife are discouraged from downloading attachments or working on non-office issued devices. When working on non office-issued devices, it is the responsibility of the concerned personnel to completely delete the electronic document containing personal data and erase any trace of the document.

A violation of this policy shall be punishable from a written warning to dismissal. In case of breach due to non-compliance with the procedures for proper disposal, the penalty shall be raised from final warning to dismissal.

POLICY FOR SOFTWARE SECURITY

Downloading or installing software on computers and electronic devices without clearance from the IT Department is strictly prohibited. Prior to installing or downloading any software, the subject member must first secure clearance with the IT Department to ensure that the software is compatible and secure.

The IT Department shall be responsible for monitoring approved software.

A violation of this policy shall be punished from Final Warning to Dismissal.

Lead
IT Department

POLICY FOR CLEAN DESK AND WORKING SPACE

All members of MBLife shall comply with the Clean Desk Policy such that every time a member is not in his/her station, it is his/her responsibility to log out his/her computer device, keep drawers under lock and key, and secure all documents or devices containing personal data.

Violation of this policy shall be penalized from Written Warning to Dismissal.

If a breach occurs as a result of a violation of this policy, the penalty shall be from Final Warning to Dismissal.

POLICY FOR USB AND EXTERNAL STORAGE DEVICES

As a general rule USB and other external storage devices are NOT allowed within the premises of MBLIfe. However, in case of need, each member bearing a USB or external storage device must register the same with the IT Department. The IT Department shall keep a logbook of a list of external storage device together with the name of the owner and contact details.

It is the responsibility of each member of the organization to monitor the presence of external storage devices within the premises. Failure by a personnel to report an unregistered external device, when found, within the premises shall be punishable from a Written Warning to Dismissal.

The IT Department shall be responsible to keep a logbook, maintain, and update the same. Failure of the IT Department to keep a logbook or to maintain or update it shall be punishable from Written Warning to Dismissal.

A violation of this provision, unless otherwise specified, shall be penalized from Written Warning to Dismissal.

Lead
IT Deparment

XVIII.
Annexes

FIGURE 1: CONSENT FORM

CONSENT FORM

We at Manila Bankers Life Insurance Corporation are committed to provide you with the services appurtenant to LIFE SAVER [insert product], while implementing safeguards designed to protect your privacy and keep your personal data safe and secure.

Processing of Personal Data
It is necessary for us collect your personal information for us to design our products to address your needs and for us to determine your eligibility for the products applied for. We use the information you provide to process your application and to service your account. Rest assured that we collect only the information necessary and we do not disclose this information to third parties.
Manila Bankers Life Insurance Corporation, as a member institution of Philippine Life Insurance Association (PLIA), is required to share your data to the Medical Interment Database of PLIA.

Data Protection
In order to protect your rights under the Data Privacy Act of 2012 (DPA), we implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collect.
The security measures enforced are directed to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful destruction, alteration, and disclosure, including unlawful processing.

Confidentiality
Our employees and agents hold your personal data under strict confidentiality. We ensure that all our employees have duly executed the necessary non-disclosure agreements and that they regularly receive training on the company's privacy and security policies to ensure confidentiality and security of personal data.

Rights and How Exercised
As a data subject, you are entitled to the rights provided for under DPA. Any information supplied by you shall not be amended without prior notice, unless otherwise provide for by law. You may exercise your rights and require access to your personal data with us upon request. Fees and related charges may apply. You may also update the information you give us by simply logging into your account, including opting in to updates on our latest products and services.

If you have further questions or concerns, you may contact our Data Protection Officer through the following channels:
Email:dpo@manilabankerslife.com
Landline:
I have read and understood this form and its contents. I consent to the processing of my personal data. I understand that my consent does not preclude the existence of other criteria for lawful processing of personal data and does not waive any of my rights under the DPA and other applicable laws. By clicking on the 'Proceed/Agree' button, I hereby grant my consent.

_____
Printed Name & Signature

FIGURE 2: PRIVACY NOTICE

PRIVACY NOTICE

The Manila Bankers Life Insurance Corporation is committed to protecting and respecting your personal data privacy. One of the ways in which we remain competitive in our industry by ensuring that we are at the forefront of compliance with the Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 and other relevant rules on data privacy.

Who We Are
Manila Bankers Life Insurance Corporation is one of the long-standing insurance companies in the Philippines. Established in 1967 and active until today, we offer life insurance products and services to our clients. In order to remain relevant in our industry today, we are offering our products and services through our website, under the guidelines provided for by the Insurance Commission on e-commerce.

Personal Information Collected
When you sign up to any of our e-commerce services, we collect information in order for us to process your application and determine your eligibility to our products. We also use your information you provide to improve our products and services. In collecting information, we collect only the information we need, encrypt them, process and store them in a secured location. We handle your personal information under a high-level obligation of confidentiality.
We collect the following information- [Please enumerate all the personal data collected]

Upon collection of personal data through this website and depending on whether or not your application is approved, we keep your personal data for a maximum period of five (5) years consistent with best industry practice from the date of termination/expiration of your account with us.

Data Sharing
Manila Bankers Life Insurance Corporation, as a member institution of Philippine Life Insurance Association (PLIA), is required to share your data to the Medical Interment Database of PLIA.
We also share your data with [Name of Company] for product and service updates. You may, however, opt out of these updates by simply updating your account with us.

Data Protection
In order to protect your rights under the Data Privacy Act of 2012, we implement reasonable and appropriate organizational, physical, and technical security measures for the protection of your personal data. Furthermore, personal data in transit is encrypted to prevent unlawful disclosure to unintended recipients. The security measures enforced are directed to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful destruction, alteration, and disclosure, including unlawful processing.
This Privacy Notice may be updated from time to time but always with prior notice to all our valued clients. Rest assured that as a valued client, we will get in touch with you through the any of the communication channel provided for in your application. If you have further questions or concerns, or if you wish to exercise your rights under the DPA, you may directly contact our Data Protection Officer:
Email:dpo@manilabankerslife.com
Landline:

Cookies Notice
We use cookies to ensure that you get the best and customized experience with our website. By proceeding, you agree to our privacy policy and accept the use of cookies. Find out more about our privacy policy here.

FIGURE 5: OUTSOURCING AGREEMENT

OUTSOURCING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This Outsourcing Agreement, herein "Agreement" is made and entered into on this 1st of January 2019 by and between:

MANILA BANKERS LIFE INSURANCE CORPORATION, a corporation duly organized and existing by virtue of the laws of the Philippines, with principal place of business at 6th Floor, VGP Center, Ayala Avenue, Makati City, represented in this act by its President and Chief Executive Office, Dr. Jose Enrique de las Peñas, hereinafter referred to as the "COMPANY";

-and-

JUAN DE LA CRUZ, of legal age and residing at _____, hereinafter referred to as the "THIRD PARTY";

RECITALS

WHEREAS, the COMPANY and the THIRD PARTY entered into a Service Agreement, a copy of which is herein attached and made an integral part of this Agreement;

WHEREAS, the COMPANY deems it in its interest to share personal data to the THIRD PARTY for its proper and efficient conduct of its obligations under the MOA;

WHEREAS, the COMPANY, in order to protect the rights of the data subjects under the MOA and in consonance with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, its implementing rules and regulations, and other relevant laws, sets forth the obligations of the THIRD PARTY with respect to the rights of data subjects;

NOW, THEREFORE, for and in consideration of the foregoing, the mutual covenants contained herein, the Parties have agreed as follows:

1. NATURE OF PERSONAL DATA. The THIRD PARTY shall fill up the required Personal Data Inventory, herein attached as Annex "A", and make them available to the COMPANY upon request. The THIRD PARTY shall ensure that the data provided for in Annex "A" shall be constantly updated in order to ensure the integrity of the data forwarded to the COMPANY.

2. DETAILS OF PERSONAL DATA. The COMPANY shall disclose personal data subject to the following guidelines-

- The quantity and coverage of personal data shared shall be directly related to, reasonable for, and proportionate to the purpose of processing. The processes to be conducted on the personal data are provided for in the MOA. The COMPANY reserves the right to limit the personal data disclosed, depending on the necessity and desirability to meet the purpose of processing;

- The COMPANY hereby grants THIRD PARTY access to the data relative to the nature of processing as declared in Annex "A";

- All personal data shares under this Agreement shall be subject to the terms and conditions of this Agreement and the MOA, the Data Privacy Act of 2012, its implementing rules and regulations, and other relevant laws as may be applicable;

- Personal data shall only be transferred and processed in accordance with relevant COMPANY security policies and always based on the documented instructions of the COMPANY, as may be approved by the Data Protection Officer or the Compliance Officer for Privacy of the COMPANY;

3. PROCESSING OF PERSONAL DATA.

- The Personal Data shall only be used by the THIRD PARTY for the singular purpose for which it was provided as stated in Annex A of this Agreement;

- The THIRD PARTY may disclose data to its employees, agents, officers, or authorized representative only to the extent that is absolutely necessary for it to fulfill its obligations under this Agreement and on a need-to-know basis. For this purpose, the THIRD PARTY shall take measures to ensure utmost confidentiality;

- The THIRD PARTY shall ensure that all employees are informed of the confidential nature of the Personal Data disclosed, have undergone appropriate training for the Data Privacy Act relating to the handling of Personal Data, and are aware the duties and obligations of the THIRD PARTY under this Agreement;

- The operational details for the use, transfer, and processing of Personal Data shall be in accordance with the MOA;

- The THIRD PARTY shall implement appropriate organization, physical, and technical security measures to protect the data from unauthorized access or disclosure. These controls include access controls, host security, business continuity plan, perimeter security, and other measures reasonably necessary to prevent any use or disclosure of personal data other than as may be permitted under this Agreement;

- The THIRD PARTY shall comply with and assist the COMPANY in ensuring compliance with applicable and relevant laws and regulations on data privacy, including the Data Privacy Act of 2012 and other issuances of the National Privacy Commission, in performing the services set out in the MOA, taking into account the nature of processing and information available to the THIRD PARTY. The THIRD PARTY must immediately inform the COMPANY in writing in the event that a process affecting personal data is not in accordance with the foregoing relevant laws and regulations;

4. TERMINATION OF THE AGREEMENT. Upon the termination of the MOA and this Agreement, the THIRD PARTY shall securely destroy and/or return all personal data in whatever form received or disclosed consistent with the security requirements agreed upon with the COMPANY. At the option of the COMPANY, the THIRD PARTY shall delete or return all personal data to the COMPANY after the end of the provision of services, unless otherwise authorized by law.

The COMPANY reserves the right to undertake audit compliance activity with the THRID PARTY in accordance with the MOA. The THIRD PARTY shall make available to the COMPANY all information necessary to demonstrate compliance with the obligations laid down in the DPA and allow for and contribute to audits, including inspections, conducted by COMPANY or a third party appointed auditor.

5. DISCLOSURES. The personal data of the COMPANY shall only be processed by the THIRD PARTY upon the documented instructions of the COMPANY, including transfer of personal data to another country or to an international organization, if authorized by law. In case of cross border personal data transfers, the geographical location of processing shall be explicitly indicated under Annex "B", herein Explicit Consent for Onward Disclosure.

THIRD PARTY shall not disclose personal data to subcontractors for the purpose of subcontracting its functions under this Agreement without the written approval from the COMPANY.
In the event that the COMPANY should permit subcontracting, the details of the outsourcing function and the purpose for each named subcontractor shall be details in Annex "B". The subcontractors shall be subject to the following conditions:

- The subcontractor shall execute an agreement with the same terms and conditions as this Agreement and the overarching MOA;

- The subcontractor shall be considered the Data Processor;

- The subcontractor shall confirm in writing that this Agreement is in place and that it has agreed to the terms and conditions under this Agreement;

- The use shall only be permitted as use stated in Annex A;

- The subcontractor shall return, destroy, or delete personal data when it no longer has a business need as may be specified in the stated purpose herein to retain it;

- The COMPANY retains the right to audit any recipient parties' compliance with the requirements of this Agreement and the requirements of the MOA. In such instances, the COMPANY shall require the THIRD PARTY to facilitate liaison with the recipient part to enable compliance checks to be carried out.

The THIRD PARTY shall ensure that any recipient of onward disclosure shall hold and handle personal data in line with this Agreement and the requirements of the MOA. Further, the THIRD PARTY shall ensure that the named subcontractors in Annex "B" are aware that the COMPANY does not grant them any rights for onward disclosure, or for uses outside of the stated purpose.

6. ONLINE SHARING OF PERSONAL DATA. The THIRD PARTY may request online access to personal data from the COMPANY. In cases where online access is allowed, the THIRD PARTY must first provide the justification and types of personal data as detailed in Annex "C", herein Online Data Sharing.

7. EFFECTIVITY. This Agreement shall be effective from the date when it is executed by both Parties. Once enforced, the data subject reserves the right to have access to this Agreement through an express communication relayed to the COMPANY as well as to the rights of a data subject as provided for in the DPA and other related rules and regulations.
In the event that the processing of personal data violates the rights of the data subject, the data subject may file a complain pursuant to the rules of filing under the DPA. In addition, any information request

or complain filed by the data subject falls under the responsibility of the COMPANY.
This Agreement shall be reviewed by both Parties annually. In certain cases, a review of this Agreement may be called for by a representative of each Party as well. This Agreement shall be in effect for one (1) year.

8. ISSUE MANAGEMENT. The unauthorized disclosure of personal data must be immediately reported by the THIRD PARTY to the COMPANY. The THIRD PARTY shall cooperate with any rectification the COMPANY, in its discretion, deems necessary to address any applicable reporting requirements and mitigate any effects of such unauthorized use or disclosure of personal data.

9. INDEMNITY. The THIRD PARTY will indemnify the COMPANY against all losses, claims, costs, expenses, and other liabilities incurred by the COMPANY as a result of or in relation to any breach of this Agreement by the THIRD PARTY or its authorized representatives.

The THIRD PARTY shall not be liable to the COMPANY nor to other third parties in case of the COMPANY's violation of laws, rules and regulations applicable to data privacy and security, even if the said violation is related to the Services rendered by the THIRD PARTY to the COMPANY, provided that the THIRD PART does not in any way contribute to the such violation.

IN WITNESS WHEREOF, the Parties hereto have affixed their signature on the date and at the place herein indicated.

FIGURE 6: NDA

Non-Disclosure Agreement

KNOW ALL MEN BY THESE PRESENTS:

This Non Disclosure Agreement, herein "NDA", is made and entered into on this __ day of November, 2018 by and between:

MANILA BANKERS LIFE INSURANCE CORPORATION, a corporation duly organized and existing by virtue of the laws of the Philippines, with principal place of business at 6th Floor, VGP Center, Ayala Avenue, Makati City, herein "FIRST PARTY"

-and-
_____, of legal age, with residence at _____, hereinafter referred to as "SECOND PARTY";

RECITALS
WHEREAS , the FIRST PARTY is a long standing life insurance corporation who has access to the Medical Information Database as approved by Insurance Commission Circular No. 2017-38;
WHEREAS, the FIRST PARTY shall provide access to the Medical Information Database (MID) to internal parties so that they may effectively perform their tasks pursuant to their employment with the FIRST PARTY;
WHEREAS, the FIRST PARTY is committed to full compliance with the requirements of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 and as such, requires the same commitment from its SECOND PARTY;
NOW, THEREFORE, for and in consideration of the foregoing and the mutual covenants contained herein, the Parties have agreed as follows:

In the performance of its duties and services under the Contract, a copy of which is herein attached and made an integral part of this NDA, SECOND PARTY accepts that the personnel it assigns shall be exposed to the personal data (including, but not limited to, billing-related information, CCTV images and recordings, complaints and disputes) of FIRST PARTY potential customers, existing clients, members, including employees("personal data"), and thus undertakes to comply with the requirements of the Data Privacy Act of 2012, its Implementing Rules and Regulations, the issuances of the National Privacy Commission, as well as the following obligations:
a. The SECOND PARTY shall process the personal data only upon the documented instructions of the FIRST PARTY, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
b. The SECOND PARTY shall ensure that an obligation of data integrity and confidentiality is imposed on persons authorized to process the personal data;
c. The SECOND PARTY shall implement appropriate security and business continuity measures, and shall allow FIRST PARTY to conduct an audit of such measures;
d. The SECOND PARTY shall not engage another processor without prior instruction from FIRST PARTY, provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
e. The SECOND PARTY shall assist FIRST PARTY, by appropriate physical, technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
f. The SECOND PARTY shall assist FIRST PARTY in ensuring compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and issuances of the National Privacy Commission, taking

into account the nature of processing and the information available to the SECOND PARTY;
g. At the choice of the FIRST PARTY, the SECOND PARTY shall delete or return all personal data to FIRST PARTY after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Data Privacy Act of 2012 or another law;
h. The SECOND PARTY shall make available to FIRST PARTY all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act of 2012, and allow for and contribute to audits, including inspections, conducted by FIRST PARTY or another auditor mandated by the latter;
i. The SECOND PARTY shall immediately inform FIRST PARTY upon knowledge of any event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data;
j. The SECOND PARTY must hold FIRST PARTY free and harmless from, and indemnify it against, any damages and liabilities arising from the breach of personal data;
k. The SECOND PARTY shall immediately inform FIRST PARTY if, in its opinion, an instruction infringes the Data Privacy Act of 2012, its Implementing Rules and Regulations, or any other issuance of the Commission.

_____
FIRST PARTY
IN WITNESS WHEREOF, the Parties have hereunto affixed their signatures on the date and at the place indicated below.

_____
SECOND PARTY

FIGURE 7: PERSONAL DATA INVENTORY

Data Subject(s):	List down all data subjects whose data is being collected by this PPPMST	Name of PPPMST:	Program, Project, Process, Measure, System or Technology that is processing the personal data listed below
Data Prepared:	_/_/____	Name of Owner:	Name of Owner

			Description of Processing			Users			Policy			
Data Elements	PI/SPI/ Priv	Source	Purpose(s)	Legal Basis	Location(s)	Internal	PIPs	Other PICs	Use/ Disclosure	Protection	Backup	Disposal
List down all data elements collected or processed												
Add more rows as needed												

FIGURE 9: DATA SHARING AGREEMENT

DATA SHARING AGREEMENT

This Data Sharing Agreement, herein "Agreement" is made and entered into on _____ 2019 by and between:

MANILA BANKERS LIFE INSURANCE CORPORATION, a corporation duly organized and existing by virtue of the laws of the Philippines, with principal place of business at 6th Floor, VGP Center, 2321 Ayala Avenue, Makati City, herein "FIRST PARTY";
-and-
ABC CORPORATION, a corporation duly organized and existing by virtue of the laws of the Philippines, with principal place of business at _____, herein "SECOND PARTY".

(The FIRST PARTY and the SECOND PARTY may each be referred to as "Party" and shall be collectively referred to as "Parties".)

RECITALS

WHEREAS, on _____, the Parties executed an agreement, herein "MOA" a copy of which is attached as Annex "A" and made an integral part of this Agreement.
WHEREAS, the Parties have established that in order for the SECOND PARTY to fulfill its obligations under the MOA, it is necessary for the FIRST PARTY to disclose data and the SECOND PARTY has assured the FIRST PARTY that it shall take all steps necessary to protect the data disclosed to it.
NOW, THEREFORE, for and in consideration of the foregoing and the mutual covenants herein set forth, the Parties have agreed as follows:

I. Purpose of Data Sharing. The Parties are entering into this Agreement and the FIRST PARTY is granting the SECOND PARTY access to the personal data described below for the following purposes:

(a) [state the purpose of data sharing]
(b)
(c)

II. Description of Personal Data

For purposes of this Agreement, the FIRST PART shall collect and share the following personal data to the SECOND PARTY for the purposes prescribed in the immediately preceding provision-

(1)
(2)
(3)

III. Consent of the Data Subject

The Parties charged with the collection of personal data directly undertake to obtain the consent of the data subject prior to collection and processing except where such consent is not required for the lawful processing of personal data as may be provided by law.
When obtaining consent, the following information may be provided to the data subject in order for the data subject to provide an express and informed consent.

(a) Identity of the PIP
(b) Purpose of Data Sharing
(c) Personal Data
(d) Intended Recipients
(e) Existence of the Rights of Data Subject

IIII. Procedures for the Use and Process of Personal Data
The Parties assure and undertake to inform the data subjects of the information stated in Article 3 prior or before personal data is shared, processed, and used.

Manner of Sharing and Processing. [how is data shared and processed] The manner of sharing and processing of data notwithstanding, shall always adhere to the data privacy principles under the Data Privacy Act of 2012, its implementing rules and regulations, and with the issuances of the National Privacy Commission.

Standard of Care. Parties to this Agreement shall always exercise the same degree of care it uses with its own personal data and confidential information, but in no case less than the reasonable care as provided by law to protect the personal data from misuse and unauthorized access or disclosure.

Safeguards. Parties to this Agreement must employ appropriate safeguards to protect the personal data from misuse and unauthorized access or disclosure, including maintaining adequate physical controls and password protections for any server or system on which the personal data is stored, ensuring that personal data is not stored on any mobile device or transmitted electronically unless encrypted, and taking any other measures reasonably necessary to prevent any use or disclosure of the personal data other than as allowed under this Agreement.

Permitted Disclosures. Parties to this Agreement may disclose personal data only to (1) the extent necessary; (2) to authorized personals; (3) with notice to the other party; and, (4) with the consent of the data subject or when otherwise expressly authorized by law.

Required Disclosures. If a party is compelled by law to disclose any personal data, it shall notify the other party in writing through its Data Protection Officer and its authorized representative of such fact before disclosing the compelled personal data.

Breach Management.
Report. Within 24 hours from notice of any unauthorized use or disclosure of the personal data or any security incident or possible security breach, a party shall promptly report such fact to the other party who shared the personal data. Both parties shall, within 72 hours from such occurrence notify the National Privacy Commission in accordance with the provisions of NPC Circular No. 16-03.

Cooperation and Mitigation. A party who received the personal data shall cooperate with any mediation that the other party, in its discretion, determines necessary to (i) address any applicable reporting requirements, and (ii) mitigate any effects of such unauthorized use or disclosure of the personal data or any security incident or possible security breach, including measures necessary to restore goodwill with stakeholders, including research subjects, collaborators, governmental authorities, and the public.
No Modification of Personal Data. A party shall NOT copy, decompile, modify, reverse engineer or create derivative works out of any of the personal data received from or share by the other party.

V. Operational Details of Personal Data Sharing.

VI. Security Measures

VII. Procedure for Online Access

VIII. Term of the Agreement
This Agreement shall be effective for a term of __ years and renewable for the same period unless otherwise terminated earlier for cause.

IX. Warranties and Representations
No Restriction. Neither party is under any restriction or obligation that could affect the performance of its obligations under this Agreement.
No Conflict. The execution or delivery of each party's obligations under this Agreement will not result in a breach of the Data Privacy Act of 2012, its IRR, and other issuances of the National Privacy Commission.
Caveat. The data provided "as is" and the FIRST PARTY does not make any warranty as to the accuracy and completeness of the data.

X. Return, Retention, Transfer, and Disposal of Transferred Data
Upon termination of this Agreement, or upon the request of the FIRST PARTY, the other party shall comply with the following-
(a) Return the personal data and any other property, information, and documents, including confidential information;

(b) Delete all personal data including confidential information provided by it, relating to the data processing and sharing;

(c) Destroy all copies made of personal data and any other property, information, and documents, including confidential information; and,

(d) Deliver to the requesting party an affidavit or certification under oath confirming the other party's compliance with the return or destruction obligation under this section.

XI. Data Protection Officer
In compliance with the Data Privacy Act of 2012, for the exercise of rights of the data subject, and for the enforcement and implementation of the provisions of this Agreement, the FIRST PARTY has designated a data protection officer which may be reached through email at dpo@manilabankerslife.com.
XII. Procedure for Requests/Complaints
For any request or complaint by a party subject to this Agreement or an affected data subject who has made a written letter, the requesting party may forward his/her request to the data protection officer stated in Article 10 of this Agreement or to the authorized representative of the relevant party.

XIII. Indemnity

The erring party shall indemnify the aggrieved part against all losses and expenses arising out of any proceeding, suit, or claim-
(a) Brought by a third party or an aggrieved party;

(b) Arising out of the party's breach of its obligations, representations, warranties, or covenants under this Agreement; and,

(c) Arising out of the defaulting party's willful misconduct or gross negligence.

XIIII. General Provisions

Security of Personal Data. Data sharing shall only be allowed where there are adequate safeguards for data privacy and security. Parties shall use contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred.
Access of the Data Sharing Agreement. A data subject, through a written request from the designated Data Protection Officer may request for a copy of this Agreement subject to reasonable fees.
Data Privacy Compliance. The Parties shall comply with the Data Privacy Act, its IRR, and all applicable issuance of the National Privacy Commission, including putting in place adequate safeguards for data privacy and security.
Confidentiality. The receiving party shall hold the other party's personal data in strict confidence. Each party will use the same degree of care to protect the data as it uses to protect its own data of like nature, but in no circumstance less than reasonable care. The receiving party shall ensure that its employees or agents are bound by the same obligations of confidentiality as the other party. The obligation of confidentiality shall be maintained even after the termination of this Agreement but shall not apply with respect to information that is independently developed by the Parties, lawfully becomes a part of the public domain, or of which the Parties gained knowledge or possession free of any confidentiality obligation.
Accountability for Cross-border Transfer of Personal Data. Each party shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.
Assignment. The Parties shall not, under any circumstances, assign and/or delegate any rights, obligations and/or duties under this Agreement unless otherwise agreed to in writing, duly signed by the authorized representatives of each Party, duly notarized and with due notice to data subjects.

Notice to the Parties. Any notice demand or claim required or permitted to be given hereunder shall be in writing and sent by registered mail, return slip requested, or by facsimile or electronic mail with verifiable answerback, or personal delivery addressed to the intended party at the following addresses, or facsimile numbers or e-mail addresses:

If to the FIRST PARTY:

MANILA BANKERS LIFE INSURANCE CORPORATION
Address:
Tel No. (02)
Fax No. (02)
E-mail:
Attention:

If to the SECOND PARTY:

ABC CORPORATION
Address:
Tel No.

Fax No.
E-mail:

Mandatory Periodic Review. The terms and conditions of this Agreement shall be subject to a mandatory review by the Parties upon the expiration of its term and any subsequent extensions thereof. The Parties shall document and include in its records:

(a) Reason for terminating the Agreement or in the alternative, for renewing its term; and,
(b) In case o renewal, any changes made to the terms and conditions of the Agreement.

Waiver. A waiver of any provision of this Agreement must be in writing and shall not be deemed a waiver of any preceding or succeeding breach of the same or of a different nature. The failure of a party at any time to require performance by the other of any provision of this Agreement shall not affect in any way the right of such party to require performance of that or any other provision; and any waiver by a party of any breach of this Agreement shall not be'-construed as a waiver of any continuing or succeeding breach of such provision, a waiver of the provision itself, or a waiver of any right under this Agreement.

Severability. Whenever possible, each provision of this Agreement will be interpreted in such a manner as to be effective and valid under applicable law, but if any provision of this Agreement is held to be prohibited by or invalid under, applicable law, such provision will be ineffective only to the extent of Such prohibition or invalidity, without invalidating the remainder of such provision of the remaining provision of this Agreement.

Governing Law. This Agreement is a contract made under the laws of the Republic of the Philippines and shall for all purposes be governed by and construed in accordance with the laws of the Republic of the Philippines.

Venue. In case of suit, the venue shall be the proper courts of Makati City, to the exclusion of all other courts.

Entire Agreement. This Agreement constitutes the complete and final agreement between parties and supersedes any and all prior agreements and negotiations between the Parties concerning the subject matter of this Agreement.

Amendment. The parties agree that no modification, change, supplement or amendment of this Agreement or any of its provisions shall be valid, unless in writing and signed by the party against whom such claimed modifications, change or amendment is sought to be enforced.

XV. Annex – Non-Disclose Agreement

IN WITNESS WHEREOF, the Parties have affixed their respective signatures on this __ day of _____, Makati City, Philippines.

MANILA BANKERS LIFE INSURANCE CORPORATION	ABC CORPORATION
By:	By:
First Party	Second Party

Signed in the presence of:

_____ _____

Republic of the Philippines)
) S.S.

ACKNOWLEDGMENT

BEFORE ME, a notary public for and in the _____ personally appeared

Name
Passport No.
Issued at
Issued on

known to me as the same persons who executed the foregoing Endorsement Agreement, consisting of ten (10) pages, including this Acknowledgement, and they acknowledged before me that the same is their free and voluntary act and deed and of the corporations and individuals they represent.

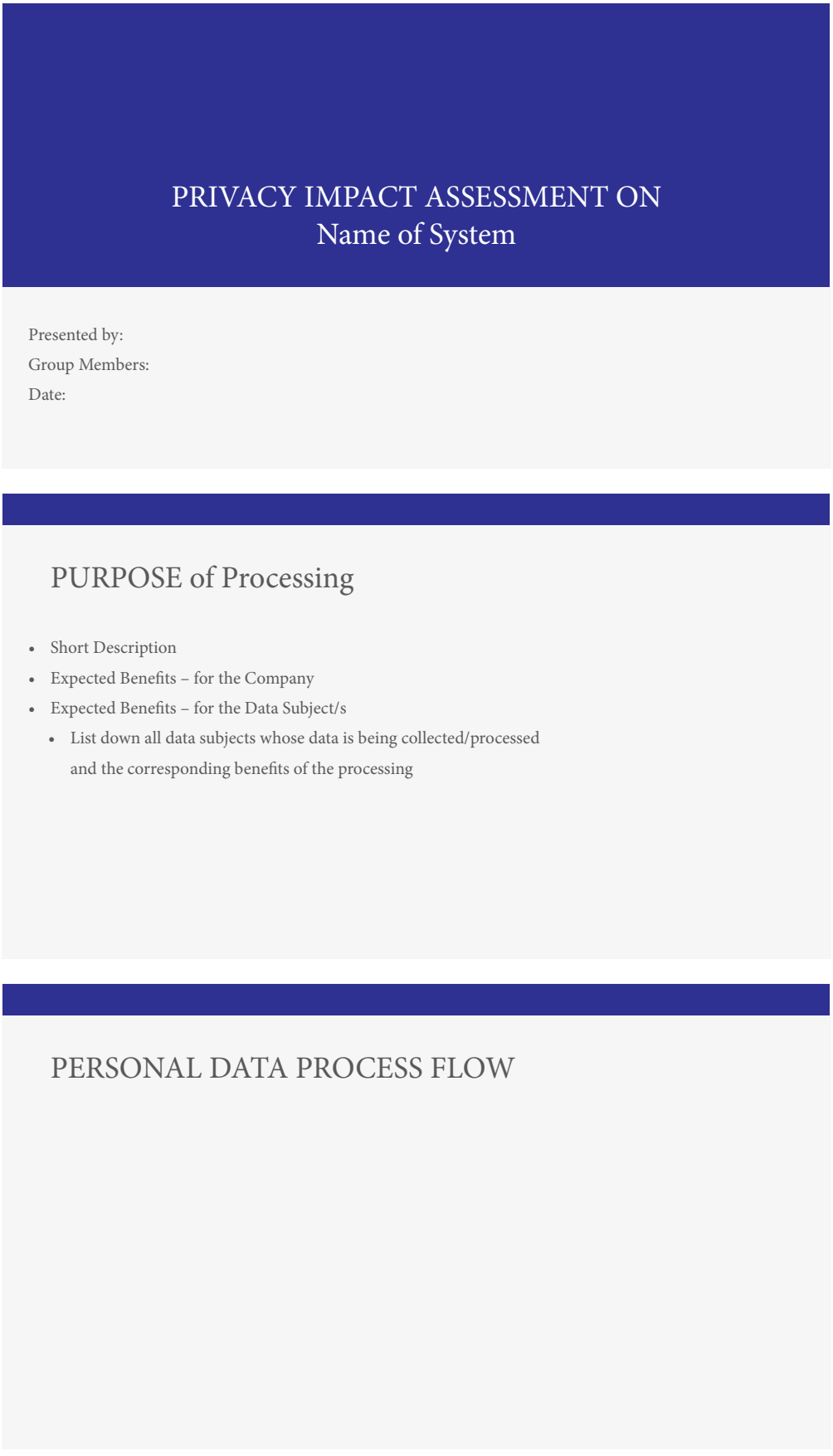
IN WITNESS WHEREOF, I have hereunto affixed my signature and notarial seal this _____ day of _____2019.

Doc. No. _____;
Page No. _____;
Book No. _____;
Series of 2019.

FIGURE 10: PERSONAL DATA INVENTORY

			Description of Processing			Users			Policy			
Data elements	PI/SPI/ Prip	Source	Purpose	Legal Basis	Locations	Internal	PIPs	Other PICs	Use/ Disclosure	Protection	Backup	Disposal

FIGURE 11: PRIVACY IMPACT ASSESSMENT SAMPLE FORMAT



STAKEHOLDERS

Third Parties and Service Providers (PIPs)

PERSONAL DATA INVENTORY

			Description of Processing			Users			Policy			
Data elements	PI/SPI/ Prip	Source	Purpose	Legal Basis	Locations	Internal	PIPs	Other PICs	Use/ Disclosure	Protection	Backup	Disposal

Information Life Cycle (Sample)

RISK IDENTIFICATION

For each privacy risk, determine the type of threat:

a. Confidentiality - disclosure to unauthorized persons

b. Integrity - accidental or intentional alteration of data

c. Availability - loss or destruction of data

d. Unauthorized - purpose or processing goes beyond what was authorized

e. Violation - privacy rights of the data subject may be curtailed or violated

Rate each privacy risk for severity or impact:

(1) Level 1 - Negligible (minor stress, irritation, annoyance

(2) Level 2 - Limited (inconvenience which can be overcome somehow)

(3) Level 3 - Significant (significant consequences, serious difficulties)

(4) Level 4 - Extreme (long-term consequences, maybe even irreversible)

Rate each privacy risk for likelihood or probability:

(1) Unlikely - very slight possibility of this happening in the future

(2) Possible - medium possibility of this happening in the future

(3) Likely - strong possibility of this happening in the future

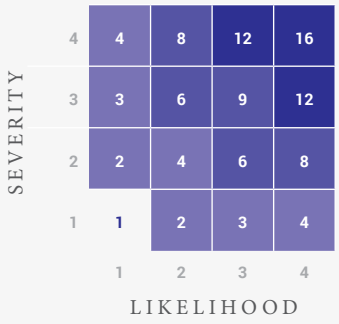
(4) Almost Certain - very high possibility of this happening in the future

RISK IDENTIFICATION

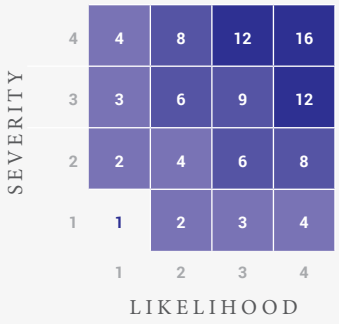
Data Subject/s who are Impacted	Possible Consequence of Privacy Risk to the Data Subject/s	Type of Threat	Severity	Likelihood

Privacy Risk Map

BEFORE CONTROLS ARE APPLIED



AFTER CONTROLS ARE APPLIED



CONTROL MEASURE TO ADDRESS RISK

Proposed Control Measures	Type of Measure (O, P, T)	Estimated Budget (PHP)	Estimated Time to Deploy

Overall Assessment/Summary

FIGURE 13: SUMMARY OF OFFENSE

Punishable Act Under Republic Act No. 10173 Otherwise Known as the Data Privacy Act of 2012	Jail Term	Fine in Pesos
25. Unauthorized Processing	1-3y to 3-6y	500,000 to 4M
26. Access Due to Negligence	1-3y to 3-6y	500,000 to 4M
27. Improper Disposal	6mos - 2y to 3-6y	100,000 to 1M
28. Unauthorized Purposes	18mos - 5y to 2-7y	500,000 to 2M
29. Intentional Breach	1-3y	500,000 to 2M
30. Concealment of Breach	18mos to 5y	500,000 to 1M
31. Malicious Disclosure	18mos to 5y	500,000 to 1M
32. Unauthorized Disclosure	1y-3y to 3y to 5y	500,000 to 2M
33. Combination of Acts	3y to 6y	1M to 5M

XIX.
Directory

Ms. Doris M. Almanzor
Chief Operations Officer
Email:
Mobile:

Atty. Rizal Antonio D. Meru
IC Compliance Officer
Email:
Mobile:

Atty. Gabriela E. Calma-Chan
Data Protection Officer
Email: dpo@manilabankerslife.com
Mobile: 0917 853 8004

Mr. Paolo Abadesco
Head of Information Technology (IT) Department
Email:
Mobile:

Atty. Maryknoll Malto
Deputy Officer for Compliance
Email:
Mobile:

MANILA BANKERS
LIFE INSURANCE CORPORATION

3/F VGP Center, 6772 Ayala Avenue, Makati City, 1223 Philippines
www.manilabankerslife.com
customercare@manilabankerslife.com
(632) 810-1040 / 810-1051 / 810-1072/ 815-1004