MAPUA UNIVERSITY
DATA PRIVACY MANUAL

Table of Contents

I. Introduction 3
II. Policy Statement 3
III. Definitions 4
IV. Scope and Limitations 7
V. Collection of Personal Information 7
A. Privacy Principles 7
i. Transparency 7
ii. Proportionality 7
iii. Legitimate Purpose 7
B. Provisions for Specific Departments 8
i. Office of Admissions and International Programs, University Registrar's Office, Center for Scholarships and Financial Aid, Center for Career Services 8
ii. Human Resources Department 8
iii. Health Services Department and Center for Guidance and Counselling 8
iv. Development Office for Information Technology 8
v. Other Departments 9
C. Privacy Policies 9
i. Data Subjects are notified and their consent secured 9
ii. Access only to Authorized Personnel 10
iii. Information is reasonably necessary and directly related to University functions or purposes 10
VI. Use and Disclosure of Information 11
i. Primary Purpose 11
ii. Secondary Purpose 11
iii. Sensitive Personal Information 11
iv. Government Related Disclosures 12
VII. Accuracy of Information 12
i. Verification Information 12
ii. Correction of Information 12
VIII. Security of Personal Information 13
A. Security Measures 13
i. Organizational Measures
ii. Information Technology 13
iii. Physical Arrangement/ Facilities 14
B. Request for Access 14
C. Retention and Destruction of Personal Information 15
IX. Inquiry, Complaints and Breach Management 15
i. Inquiry on Data Privacy Issues 15
ii. Procedure for Complaints and Breach Management 15
Disclosure or Destruction of Personal Information
X. Privacy Impact Assessments 17
XI. Effectivity 17
XII. Annexes 18
i. Data Privacy Act of 2012 18
ii. Implementing Rules and Regulations 36

I. INTRODUCTION

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

It is the policy of Mapua to respect and uphold data privacy rights, and to ensure that all personal data collected from students, their parents or guardians, employees and other third parties, are processed pursuant to the general principles of transparency, legitimate purpose, and proportionality as stated in DPA.

This Manual outlines the data protection and security measures adopted by the University to protect data privacy rights, and shall serve as a guide in the exercise of rights under the DPA.

II. POLICY STATEMENT

Mapua University is committed to protect the privacy rights of individuals on personal information pursuant to the provisions of Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations and the Basic Education Act of 1982.

All employees, students and administration officers are enjoined to comply with and to share in the responsibility to secure and protect personal information collected and processed by Mapua in pursuit of legitimate purposes.

General Privacy Policy Statements

1. Mapua adheres to the general principles of transparency, legitimate purpose and proportionality in the collection, processing, securing, retention and disposal of personal information.
2. The students, parents, guardians, employees or third parties whose personal informationis being collected shall be considered as data subjects for purposes of these policies.
3. Data subjects shall be informed the reason or purpose of collecting and processing of personal data.
4. The data subjects shall have the right to correct the information especially in cases of erroneous or outdated data, and to object to collection of personal information within the bounds allowed by privacy and education laws.
5. The data subject has the right to file a complaint in case of breach or unauthorized access of his personal information.
6. Mapua shall secure the personal information of students, parents, guardians, employees and third parties from whom personal information is collected and shall take adequate measures to secure both physical and digital copies of the information.

7. Mapua shall ensure that personal information is collected and processed only by authorized personnel for legitimate purposes of the University.
8. Any information that is declared obsolete based on the internal privacy and retention procedures of the University shall be disposed of in a secure and legal manner.
9. Any suspected or actual breach of the Mapua Data privacy policy must be reported to any member of the Data Privacy Response Team in accordance with the procedure provided in Article IX (ii) of this Manual.
10. Data subjects may inquire or request for information from the Data Privacy Response Team, regarding any matter relating to the processing of their personal data under the custody of Mapua, including the data privacy and security policies implemented to ensure the protection of their personal data pursuant to Article IX (i) of this Manual.

III. DEFINITIONS

A. "**Authorized personnel**" refers to employees or officers of the University specifically authorized to collect and/ or to process personal information either by their function of their office or position, or through specific authority given in accordance with the policies of the University.

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

C. "**Data subject**" refers to an individual whose personal, sensitive personal, or privileged information is processed. For purposes of this Manual, students, employees and third parties whose information is being collected and processed by the University (i.e. applicants for admission or employment, former students or alumni whose records are required by law to be kept and maintained by the University). The Data subjects have the right to be informed [Article V Section C (i)] and object or complain [Article IX ii and ii], right to access [Article VIII (B)] their individual information, and the right to correct, rectify or block [Article VII (I and ii)] any erroneous or false information.

D. "**Data Privacy Officer or DPO**" refers to the University officer designated to monitor and ensure the implementation of the Data Privacy policies of the University. The DPO is also the de facto head of the Data Privacy Response Team.

E. "**Data Privacy Response Team**" refers to the group of persons designated to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policy of the University. The Mapua Data Privacy Response Team is composed of the Data Privacy Officer and the Personal Information Processors. The contact details of team is contained in Article IX of this Manual.

F. "**Personal data**" refers to all types of personal information collected and processed by the University from the data subjects.

G. "**Personal data breach**" refers 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.

H. "**Personal Data Classification**" refers to the *categories of personal information* collected and processed by Mapua. Personal data is classified as follows

   a. **Public**- these are information readily available and may be disclosed to the public. Examples: Mapua offices directory, course catalogs, program offerings, names of officers, deans and faculty as stated in the Administration portion of the Mapua website, published research containing the names of faculty members and students
   b. **Confidential**- Those which are declared confidential by law or policy of Mapua, and which may only be processed by authorized personnel, and if disclosed may cause material harm to the University, or information is sensitive in nature as will affect the health or well-being of the individual.
      Examples: Employee and student names, addresses, contact numbers, SSS, PhilHealth, Passport numbers, student and employee's health information, student counselling and medical records (Data Privacy Law); financial information of parents and students and employees, and student records (MORPHE), Employee 201 files and the information contained therein (Labor Code)
   c. **Classified**- These are information the access of which is highly restricted, and if disclosed may cause severe or serious harm or injury to the employee, student or third party.
      Examples: Employee and student my mapua account or computer passwords (Data Privacy Law, Anti-Cyber Crime Law, Mapua IT policies), bank account numbers, PIN numbers of employee and student ATM's.

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

J. "**Personal Information Controller or PIC**" refers to the University as the entity which controls of the processing of personal data, or instructs another to process personal data on its behalf.

K. "**Personal Information Processor or PIP**" refers to the University Officer person designated as such to whom the personal information controller instructs the processing of personal data pertaining to a data subject.

L. "**Privacy Impact Assessment**" refers to the process undertaken and used to evaluate and manage the impacts on privacy of University programs, projects, processes, measures, systems, or technology products. Such process takes into account the nature of the personal data to be

protected, the personal data flow. The risks to privacy and security posed by the processing, current data best practices, cost of security implementation, and where applicable, the size of the organization, its resources and complexity of operations.

M. "**Processing**" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, 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.

N. "**Privacy Statement"** is a notification or statement, in the format specified under Section 5.1 (i) of this Manual provided to an individual informing them of the use and purpose for collecting or processing the information, and/or which allows such individual to consent to such processing of information.

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

P. "**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;

Q. "**Sensitive personal information**" refers to personal information about:

i. an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations.
ii. 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.
iii. issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns
iv. Specifically established by an executive order or an act of Congress to be kept classified.

R. "**School records**" refer to the records of students of all acts, events, accomplishments, results or research and all documents depicting the various activities of the students. This include but are not limited to the following:

i. Personal and academic records of the student
ii. Baptismal and Birth Certificates
iii. Academic reports
iv. Medical and Guidance Records
v. Disciplinary records
vi. Alien Certificate for foreign students
vii. Individual financial records (i.e. individual tuition fee payments, balances etc.)

S. "**University personnel**" means all employees (regardless of the type of employment or contractual arrangement) of the University.

IV. SCOPE AND LIMITATIONS

This Manual applies to all departments of the University, employees regardless of the type, students, officers and third parties whose information (applicants for admission or employment and former students or alumni whose school records are required to be kept and secured by the University. The data covered by this Manual is limited to **personal information as defined under Section III (I), collected and processed** by the University.

This Manual is reviewed annually and updated regularly to comply with the current data privacy laws, policies and regulations.

V. COLLECTION OF PERSONAL INFORMATION

A. Privacy Principles espoused by the University

i. TRANSPARENCY. Data Subject's consent should be obtained before collecting the information and the latter should be informed of the purpose for which the information is to be collected.

Example: In the enrolment process, upperclassmen are required to fill out the Student Data Sheet. The purpose of such collection of information is stated in the form and the consent of the student is obtained through the form which is filled out and signed by the student.

ii. **PROPORTIONALTY**. Personal Information collected must be reasonably necessary or directly related to the University's functions

Example: In the application for admission as a college student in Mapua, only information such as name, address, contact numbers, previous schools, parent's or guardian's name, which necessary for the evaluation for eligibility for admission to the University is collected.

iii. **FOR LEGIMATE PURPOSE.** In collecting personal information, the University shall use the information only for legitimate purposes as discussed in Section VI of this Manual

Example: Personal information such as student's name, parents name and addresses and contact numbers etc., shall be used only for purposes such as enrolment, academic activities and availment of student services which is allowed under the provisions of the Manual of Regulations for Private Higher Education.

B. Provisions for Specific Departments

i. Office of Admissions, University Registrar's Office, Center for Career Services and Center for Scholarships and Financial Assistance

The Office of Admissions and the University Registrar's Office collects personal information for the purpose of evaluating the eligibility of the applicant for admission or in case of current students, for enrollment in the University.

The Center for Career Services and Center for Scholarships are tasked to collect personal information only for the purpose of providing placement services for required on the job training for students, and evaluation of students for eligibility for scholarships provided by the University and third parties.

In the course of the collection of information, these authorized personnel from these offices ask data subjects (students and their parents or guardians and to fill out forms with the corresponding privacy statement to signify consent and to inform them of the purpose of collecting such information during the admission and/ or enrollment processes). These departments collect, process the information and encode the same in the Student (profile) Data base. Only authorized personnel are allowed to encode and access student data.

Access is restricted pursuant to the provisions of the Manual of Regulations for Private Higher Education (MORPHE) which specifically provides that all student records should be kept confidential.

ii. Human Resources Department

The Human Resource Department collects the information from employees or applicants for purposes of evaluating the applicant for eligibility for employment, and availment of employee benefits (i.e. retirement, educational and medical benefits) and collates the information in the individual 201 files of the employees which is required under the provisions the Labor Code.

Pursuant to existing labor laws and human resources policies of the University, the 201 files or employee's individual employment records are confidential and access is restricted to authorized personnel only.

iii. Health Services Department and Center for Guidance and Counselling

The Health Services Department collects sensitive information relating to the medical and dental health of students for monitoring pursuant to the provisions of the Manual of Regulations for Private Higher Education.

Access to the data collected is restricted and limited only to authorized personnel in the department such as the school doctor, dentist or nurse assigned in the Department. Sensitive information may not be released without the prior consent of the student or guardian except in

cases life of the student or other students (i.e. epidemic cases as provided under the DOH rules and regulations) is at stake.

iv. Development Office for Information Technology

The Development Office for Information Technology is tasked to process, secure and store the information and data base systems in the University. All personal information collected from students by the different departments mentioned above are primarily encoded and stored in the Student Records Management System. Employee personal information collected by the HRD is encoded and stored in the Human Resources Information System.

Access to the data is also restricted and given only to predetermined authorized personnel in relation to their specific function which requires them to access or process student or employee information. In all instances, any access to personal information of students must be with their or their parents/ guardians' consent, or employee's and for legitimate purposes, or endorsed by the Department head, and approved by the DO-IT Head or his authorized representative.

v. Other Departments

All other departments who collect, process or store student or employee personal information, if any, are subject to the policies provided under this Manual. Department heads are responsible for ensuring compliance of the provisions of this Manual within their departments.

C. Privacy Policies

To ensure that the rights of the data subjects are protected, the above-mentioned departments are subject to the following policies:

i. Data Subjects are notified and their consent secured

Collection of information is done with the consent of Data Subjects (Students and their guardians) which consent is included in the forms filled-out during application for admission, enrollment or availment of student services such as scholarships, on the job trainings, etc.

Forms for collection of personal information include a provision or a variation of these privacy statements:

> "All information shall be used by the University for legitimate purposes specifically for_____and shall be processed by authorized personnel in accordance with the Data Privacy Policies of the University."

> "I hereby allow/authorize Mapua to use, collect and process the information for legitimate purposes specifically for _____, and allow authorized personnel to process the information."

In case, there is no form or written document containing the privacy statement, the authorized personnel tasked to collect the information may verbally notify them of the purpose and ask the Data Subject to allow the University personnel to collect and process the information and shall record the processing of information with consent in writing.

ii. Access only to Authorized Personnel

Only authorized personnel are allowed to access and process the personal information collected from the students, their parents or guardians in accordance with Data Privacy policies of the University and the MORPHE which requires that student records as well as the information contained therein are to be kept confidential.

> Example: Only the registrar or her duly authorized representative or personnel is allowed complete access to the student profile which includes the name, student number, parents names, addresses, contact numbers, grades etc.

iii. Information is reasonably necessary and directly related to University functions or purposes

Authorized university personnel shall collect personal information which is reasonably necessary or directly related to the University's primary or secondary functions or activities. Personal Information shall not be collected in anticipation that it may be useful in the future ("just in case" it is needed). The physical records or those which are not digital stored and secured in the Mapua data base are stored in the particular offices of the each Department. For student records from previous years which are required to perpetually stored and maintained by the University, a warehouse in a secured location is maintained by a third party tasked to physically store and secure the records. Access is restricted where such records may only be retrieved upon specific instructions of the University Registrar and only for legitimate purposes or upon request of the student or alumni for copies of their individual school record or pursuant to the University Registrar's procedures and policies on request for records.

Personal information shall be collected by lawful and fair means, which is allowed under the University's policies and the provisions of the MORPHE.

> Example: For foreign students, nationality, ACR numbers, passport numbers and the contact numbers of the parents are guardians are necessary in case of emergencies and other situations where the student's parents or embassy are required to be notified.

VI. USE AND DISCLOSURE OF INFORMATION

Authorized university personnel are allowed to access, use and process said information for legitimate primary or secondary purposes of the University and/or that which is stated in the privacy statement contained in the forms or documents signed by the students, third parties or employees.

i. Primary Purpose

As an educational institution, personal information is collected primarily for the educational purposes of the students and employment purposes. This includes monitoring academic activities as well as extracurricular activities of students, pursuant to the MORPHE, and monitoring potential and current employees in accordance with labor laws. This also includes information collected for purposes set out in the privacy statements contained in the documents signed by students or employees. Such information is allowed to be processed and used by authorized personnel for such purposes.

ii. Secondary Purposes

Secondary purposes are those which are collateral to the primary purposes and which are necessary to process the information. This include monitoring the current administrative or disciplinary standing (for student and employee discipline), financial condition (for scholarship purposes) or the health and psychological wellness of students and employees (health purposes). Authorized university personnel are allowed to use personal information collected and/or processed for such purposes provided the following circumstances are present:

a. the student or employee has consented to the use or disclosure for the secondary purpose; **or**
b. the student or employee would reasonably expect the University through its authorized personnel to use, or process personal information for secondary purpose **and** that the secondary purposes are directly related to the primary purposes; or

iii. Sensitive Personal Information

Sensitive personal information may not be disclosed or processed, except in any of the following cases:

a. Consent is given by data subject, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose of the University.
b. The processing of the sensitive personal information provided for by existing laws and regulations, such as medical history required under the MORPHE to be disclosed by the student as part of the monitoring of the health of the student, provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data.

c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing.
d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that the processing is confined and related to the bona fide members of these organizations or their associations; the sensitive personal information are not transferred to third parties; and consent of the data subject was obtained prior to processing.
e. The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured.
f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

iv. Government-Related Use and Disclosures

Personal information is allowed to be used and disclosed to government agencies to satisfy reportorial requirements in line with their constitutionally or legislatively mandated functions pursuant to existing education or labor laws or when the use of pursuant to lawful order of a court or tribunal.

VII. ACCURACY OF INFORMATION

i. Verification of information

Authorized university personnel must take reasonable steps to ensure that the personal information collected or processed, up-to-date, complete, relevant and not misleading.

The information collected from students and employees is verified by the particular departments collecting the information. Student information is verified by the University Registrar's Office while the HRD conducts the verification of employee information and background checks.

ii. Correction, or update of information

Students may update their personal information through forms available from the University Registrar's Office, or in their respective Schools, while for employees they may write to or directly go to the HRD Office to update their information**.** In case of erroneous or false information, the students or employees may have the information corrected, rectified, blocked or erased (blocking and erasure only to the extent allowed by MORPHE and other applicable laws) using the same process.

VIII. SECURITY OF PERSONAL INFORMATION

A. Security Measures

i. Organizational Measures

a) Appointment of Data Privacy/Protection (DPO) and Data Privacy Response Team

In line with the University's mandate to comply with the DPA and its IRR to secure the personal information of its students, parents, employees and third parties, the University has designated its Data Privacy/Protection Officer (DPO) who is tasked to designated to monitor and ensure the implementation of the DPA and its IRR and the Data Privacy policies of the University. Members of the Data Privacy Response Team were also designated. The DPO is the de-facto head of the Data Privacy Response Team which is tasked to respond to inquiries and complaints relating to data privacy and to assist in the monitoring and implementation of the Data Privacy policy of the University.

b) Institutional Data Privacy Manual

The University has data privacy policies are contained in the institutional Data Privacy Manual which is reviewed annually and regularly updated.

c) Conduct of Awareness Campaign and Data Privacy Trainings

The University regularly conducts awareness campaigns and data privacy trainings as part of its commitment to ensure that all its students and employees comply with its data privacy policies.

d) Conduct of Privacy Impact Assessments

To ensure that the potential privacy impact of the University's processes, information system programs and other initiatives which process personal information of students, employees and third parties are evaluated, privacy impact assessments are conducted for such projects, programs and initiatives.

ii. Information Technology

The University shall take reasonable steps to protect the personal information in its possession from misuse, loss or unauthorized access, modification or disclosure.

As most of the personal information of students and employees are stored in the University data bases, access to personal information in digital or digitized form by authorized IT personnel is restricted and individually identifiable. An approval process is in place for internal requests (i.e. special requests for authority to view student profile for disciplinary cases, counselling, or health concerns) for access to restricted student or employee records contained in the University information systems. As a general rule only authorized personnel

with the necessary approvals may request for access of the information systems of personal information in accordance with the procedure established by DOIT, and Article VIII (B) of this Manual.

Physical access to the servers and network equipment is highly restricted to authorized personnel only. Various security appliances, devices and measures are employed to safeguard the university network and its systems. For third party providers of programs, applications and platforms, the University ensures that they have adequate security devices and measures and policies to ensure secure access, and they comply with the University data privacy policies. Contract provisions on data privacy are also included on the agreements to ensure compliance.

24-hour security is also provided by the University to secure the areas where the University data centers are located.

iii. Physical Arrangement/Facilities

Access to student and employee personal information is limited to authorized personnel of the specific departments collecting or processing the information.

Aside from access restriction, the storage facilities for the hard copies of documents containing personal information are also secured (i.e locked) in cabinets or storage facilities. Only authorized personnel can open or have access to keys to the storage facilities. The storage units or facilities are placed in areas which are not usually accessible to the public, safe from physical hazards such as rain, wind and dust, and located in areas which are usually manned by the authorized personnel.

Round the clock security is also provided for the entire University including areas where the hard copies of such documents are kept and secured.

B. Request for Access

As a general rule, only authorized personnel shall have access to student or employee personal information. Students or parents or guardians (in case of minors) who wish to have access to their own personal information may submit a written request directly to the Registrar's Office and may be allowed access to their specific individual information or given copies, pursuant to the policies and guidelines on requesting for access or copies of student records. Request for information through telephone is not allowed. In case of email inquiry, proof of actual parent or student identity shall be submitted along with the email request.

Employees who wish to view the personal information in their individual personnel file may file a written request or directly go to the HRD Office, and request for viewing of such information in the presence of an authorized personnel of the department.

As a general rule only authorized personnel may be allowed to have access to the personal information subject to the procedure established in this section. In such cases where any individual or entity [other than the student, parent or guardian in case of minors, or employee] wishes to have access pursuant to the instances or exceptions provided under Data Privacy Act or Article VI of this Manual, a written request shall be submitted to the Department Head who

may either endorse or reject the same. If approved, the endorsed request shall be submitted to the DPO or her duly authorized representative for approval. If the request involves digital or digitized data, then the approval of the DOIT Director is required prior to endorsement of the Department Head to the DPO. Only written requests properly endorsed by the Department Head shall be considered for approval.

The written request shall state the name of the requestor, the purpose, the type of access requested (i.e. copying or viewing only), and the time frame or time limit within which access shall be given with a guarantee that the information shall be used solely for purposes allowed by law and a statement that such shall be treated with utmost confidentiality.

In cases where government agencies empowered under the law to request for personal information (i.e. BIR, DOH), request for access, university personnel must ensure that the request is in writing, citing the authority upon which the request is made. In cases where the request is a result of a valid order or decision of a tribunal or court, a copy of such order shall be attached to the written request.

Once approved by the DPO, it shall be transmitted to the Department Head or appropriate Department for implementation.

The Department Head who endorsed the same shall be responsible for monitoring compliance of the requestor on the terms of the approved request (i.e time limit and confidentiality).

In case there is doubt on the propriety of any request for access, university personnel should consult or seek clearance from the Legal Affairs Department or the DPO.

C. Retention and Destruction of Personal Information

Under the provisions of the MORPHE and existing Labor laws, the University is required to permanently keep the student and employee records including the information contained therein. In line with this, no personal information may be destroyed unless allowed by such laws, and such destruction, if allowed or authorized by law and the University, must be documented in writing by the University. Unauthorized destruction should be reported to the DPO or any member of the Data Response Team pursuant to the procedure stated in the succeeding section.

IX. Inquiry, Complaints and Breach Management

i. Inquiry on Data Privacy issues

Data subjects may inquire or request for information from the Data Privacy Response Team, regarding any matter relating to the processing of their personal data under the custody of Mapua, including the data privacy and security policies implemented to ensure the protection of their personal data.

ii. Procedure for Complaints and Breach Management

Any suspected or actual breach of the Mapua Data privacy policy, violation of data privacy rights, or any breach, loss or unauthorized access or disclosure of personal information in the possession or under the custody of the University must be reported immediately to the any member of the Data Privacy Response Team.

In case of a complaint for violation of the Mapua Data Privacy Policies as contained in the provisions of this Manual, or any serious breach, loss or unauthorized access, disclosure or destruction of personal information in the possession or under the custody of the University and within reasonable time, the DPO or any (2) members of the Privacy Team shall conduct a verification of the allegations in the complaint, and if warranted, and an official investigation in cases of serious security breach as provided under Republic Act No. 10173 or the Data Privacy Act of 2012 and its Implementing Rules and Regulations Act, and shall report the same to the National Privacy Commission within seventy-two (72) hours from knowledge thereof, and in cases of breach of personal data, the DPO shall initiate the breach management procedure as provided in the policies of the University which includes conducting an investigation on the matter, risk assessment, containment, recovery and recommendation on permanent corrective measures

The DPO may also convene the entire team in case of a complaint, or *motu-propio* in case the violation of policies or data breach, loss, unauthorized access or destruction as an investigation committee to recommend actions, particularly when the violation is serious or causes or has the potential to cause material damage to the University or any of its students or employees. Such recommendation shall be submitted to the President of the University for approval. Any appeal on such approved recommendation/Decision shall be made by any of the affected parties within 15 days from receipt of the approved Decision.

Mapua Data Privacy Response Team

Atty. Denise Jordan P. Arenillo
Data Privacy/Protection Officer
Tel No. 8527-1658/ 5247-5000 local 8011
E-mail address: mapuadpo@mapua.edu.ph

Margarita V. Camacho
Personal Information Processing Officer
Tel No. 8247-5000 local 1201/ 5336-7105
E-mail address: mvcamacho@mapua.edu.ph

Ariziel Ruth D. Marquez
Personal Information Processing Officer
Tel No. 8527-3680/ 8247-5000 local 5053
E-mail: ardmarquez@mapua.edu.ph

Ma. Elizabeth S. Yap
Personal Information Processing Officer
Tel No. 8247-5000 local 1305
E-mail address: mesyap@mapua.edu.ph

X. PRIVACY IMPACT ASSESSMENTS

To assess the potential privacy impact of the University's processes, information system programs and other initiatives which process personal information of students, employees or third parties in consultation with the University stakeholders, privacy impact assessments shall be conducted prior to implementation to identify and minimize potential privacy risks .

The privacy impact assessment shall include the following:

i. systematic description of the process, nature, scope, context and the purposes of the processing, including, where applicable, the legitimate interest pursued by University;
ii. assessment of the necessity, proportionality of the processing operations in relation to the purposes and compliance measures;
iii. identification and assessment of the risks to the rights and freedoms of data subjects;
iv. identification and additional measures to be placed to address and mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with DPA, its IRR and the University Data Privacy policies into account the rights and legitimate interests of data subjects and other persons concerned.

Privacy impact assessments conducted for Mapua processes or projects shall be evaluated by the DPO and shall be submitted to the President for approval.

XI. EFFECTIVITY

The provisions of this revised Manual shall take effect on August 15, 2017.

XII. ANNEXES

A. Data Privacy Act of 2012

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *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 personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

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

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

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

(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(l) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

(j) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

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

(l) *Sensitive personal information* refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided,* That the requirements of Section 5 are complied with.

This Act does not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic, literary or research purposes;

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise

known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

SEC. 5. *Protection Afforded to Journalists and Their Sources.* – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.

SEC. 6. *Extraterritorial Application.* – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

CHAPTER II
THE NATIONAL PRIVACY COMMISSION

SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: *Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: *Provided, further,* That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory

agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;

(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

SEC. 8. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made.

The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.

The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: *Provided,* That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

SEC. 10. *The Secretariat.* – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

CHAPTER III
PROCESSING OF PERSONAL INFORMATION

SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must, be:

(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed fairly and lawfully;

(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing principles set out herein.

SEC. 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

SEC. 14. *Subcontract of Personal Information. – A* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

SEC. 15. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

(1) Description of the personal information to be entered into the system;

(2) Purposes for which they are being or are to be processed;

(3) Scope and method of the personal information processing;

(4) The recipients or classes of recipients to whom they are or may be disclosed;

(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

(6) The identity and contact details of the personal information controller or its representative;

(7) The period for which the information will be stored; and

(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided,* That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c)) Reasonable access to, upon demand, the following:

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 17. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 18. *Right to Data Portability.* – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

SEC. 19. *Non-Applicability.* – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: *Provided,* That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

CHAPTER V
SECURITY OF PERSONAL INFORMATION

SEC. 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal

information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.

(2) The Commission may exempt a personal information controller from notification where, inits reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

CHAPTER VI
ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

CHAPTER VII
SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

SEC 22. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

SEC. 23. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by

the Commission, no employee of the government shall have access to sensitive personal information on government propertyor through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;

(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and

(3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 24. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

CHAPTER VIII
PENALTIES

SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 27. *Improper Disposal of Personal Information and Sensitive Personal Information.* – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information ofan individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shallbe imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

SEC. 29. *Unauthorized Access or Intentional Breach.* – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on

persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

SEC. 30. *Concealment of Security Breaches Involving Sensitive Personal Information.* – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

SEC. 31. *Malicious Disclosure.* – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 35. *Large-Scale.* – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

CHAPTER IX
MISCELLANEOUS PROVISIONS

SEC. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

SEC. 39. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 40. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 41. *Appropriations Clause.* – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

SEC. 42. *Transitory Provision.* – Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.

In case that the DICT has not yet been created by the time the law takes full force and effect, the National Privacy Commission shall be attached to the Office of the President.

SEC. 43. *Separability Clause.* – If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid andsubsisting.

SEC. 44. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 45. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Approved,

(Sgd.) **FELICIANO BELMONTE JR.** *Speaker of the House of Representatives*	(Sgd.) **JUAN PONCE ENRILE** *President of the Senate*

This Act which is a consolidation of Senate Bill No. 2965 and House Bill No. 4115 was finally passed by the Senate and the House of Representatives on June 6, 2012.

(Sgd.) **MARILYN B. BARUA-YAP** *Secretary General* *House of Representatives*	(Sgd.) **EMMA LIRIO-REYES** *Secretary of the Senate*

Approved: **AUG 15 2012**

(Sgd.) **BENIGNO S. AQUINO III** *President of the Philippines*

B. Implementing Rules and Regulations of the Data Privacy Act of 2012

Republic of the Philippines

National Privacy Commission

Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012

Pursuant to the mandate of the National Privacy Commission to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection, the following rules and regulations are hereby promulgated to effectively implement the provisions of the Act: Rule I. Preliminary Provisions

1. Title
2. Policy
3. Definitions

Rule II. Scope of Application

4. Scope
5. Special Cases
6. Protection afforded to data subjects
7. Protection afforded to journalists and their sources

Rule III. National Privacy Commission

8. Mandate
9. Functions
10. Administrative Issuances
11. Reports and Public Information
12. Confidentiality of Personal Data
13. Organizational Structure
14. Secretariat
15. Effect of Lawful Performance of Duty
16. Magna Carta for Science and Technology Personnel

Rule IV. Data Privacy Principles

17. General Principles
18. Principles of Transparency, Legitimate Purpose and Proportionality
19. Principles in Collection, Processing and Retention
    a. Collection must be for a specified and legitimate purpose
    b. Personal Data shall be processed fairly and lawfully
    c. Processing should ensure data quality

d. Personal data shall not be retained longer than necessary
e. Any authorized further processing shall have adequate safeguards

20. Principles for Data Sharing

Rule V. Lawful Processing of Personal Data

21. Lawful Processing of Personal Information
22. Lawful Processing of Sensitive Personal Information and Privileged Information
23. Extension of Privileged Communication
24. Surveillance of Subjects and Interception of Recording of Communications

Rule VI. Security Measures for Protection of Personal Data

25. Data Privacy and Security
26. Organizational Security
27. Physical Security
28. Technical Security
29. Appropriate Level of Security

Rule VII. Security of Sensitive Personal Information in Government

30. Responsibility of Heads of Agencies
31. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
32. Implementation of Security Requirements
33. Applicability to Government Contractors

Rule VIII. Rights of Data Subject

34. Rights of the Data Subject
    a. Right to be informed
    b. Right to object
    c. Right to access
    d. Right to correct
    e. Right to rectification, erasure or blocking
35. Transmissibility of Rights of the Data Subject
36. Right to Data Portability
37. Limitation on Rights

Rule IX. Data Breach Notification.

38. Data Breach Notification
39. Contents of Notification
40. Delay of Notification
41. Breach Report
42. Procedure for Notification

Rule X. Outsourcing and Subcontracting Agreements.

43. Subcontract of Personal Data
44. Agreements for Outsourcing
45. Duty of Personal Information Processor

Rule XI. Registration and Compliance Requirements

46. Enforcement of the Data Privacy Act
47. Registration of Data Processing Systems
48. Notification for Automated Processing Operations
49. Review by the Commission

Rule XII. Rules on Accountability

50. Accountability for Transfer of Personal Information
51. Accountability for Violation of the Act, these Rules and other issuances

Rule XIII. Penalties

52. Unauthorized Processing of Personal Information and Sensitive Personal Information
53. Accessing Personal Information and Sensitive Personal Information Due to Negligence
54. Improper Disposal of Personal Information and Sensitive Personal Information
55. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
56. Unauthorized Access or Intentional Breach
57. Concealment of Security Breaches Involving Sensitive Personal Information
58. Malicious Disclosure
59. Unauthorized Disclosure
60. Combination or Series of Acts
61. Extent of Liability
62. Large-Scale
63. Offense Committed by Public Officer
64. Restitution
65. Fines and Penalties

Rule XIV. Miscellaneous Provisions

66. Appeal
67. Period for Compliance
68. Appropriations Clause
69. Interpretation
70. Separability Clause
71. Repealing Clause
72. Effectivity Clause

Rule I. Preliminary Provisions

Section 1. *Title*. These rules and regulations shall be known as the "Implementing Rules and Regulations of the Data Privacy Act of 2012", or the "Rules". Section 2. *Policy*. These Rules further enforce the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection. They safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. These Rules also recognize the vital role of information and communications technology in nation-building and enforce the State's inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected. Section 3. *Definitions*. Whenever used in these Rules, the following terms shall have the respective meanings hereafter set forth:

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

b. "Commission" refers to the National Privacy Commission;

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

d. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

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

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

g. "Direct marketing" refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals;

h. "Filing system" refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to

individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

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

j. "Personal data" refers to all types of personal information;

k. "Personal data breach" refers 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;

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

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

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

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

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

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

o. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, 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;

p. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular

to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

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

r. "Public authority" refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

s. "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;

t. Sensitive personal information refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. About an individual's health, education, 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;

3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

4. Specifically established by an executive order or an act of Congress to be kept classified.

Rule II. Scope of Application

Section 4. *Scope*. The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector. They apply to an act done or practice engaged in and outside of the Philippines if:

a. The natural or juridical person involved in the processing of personal data is found or established in the Philippines;

b. The act, practice or processing relates to personal data about a Philippine citizen or Philippine resident;

c. The processing of personal data is being done in the Philippines; or

d. The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, such as, but not limited to, the following:

1. Use of equipment located in the country, or maintains an office, branch or agency in the Philippines for processing of personal data;

2. A contract is entered in the Philippines;

3. A juridical entity unincorporated in the Philippines but has central management and control in the country;

4. An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;

5. An entity that carries on business in the Philippines;

6. An entity that collects or holds personal data in the Philippines.

Section 5. *Special Cases*. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

a. Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:

1. Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:

(a) The fact that the individual is or was an officer or employee of the government;

(b) The title, office address, and office telephone number of the individual;

(c) The classification, salary range, and responsibilities of the position held by theindividual; and

(d) The name of the individual on a document he or she prepared in the course of his or her employment with the government;

2. Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract;

3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit: Provided, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

b. Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;

c. Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;

d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

e. Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas, and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws;

f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules:

Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity. Section 6. *Protection afforded to Data Subjects*.

a. Unless directly incompatible or inconsistent with the preceding sections in relation to the purpose, function, or activities the non-applicability concerns, the personal information controller or personal information processor shall uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.

b. The burden of proving that the Act and these Rules are not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability.

c. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

Section 7. *Protection Afforded to Journalists and their Sources.*

a. Publishers, editors, or duly accredited reporters of any newspaper, magazine or periodical of general circulation shall not be compelled to reveal the source of any news report or information appearing in said publication if it was related in any confidence to such publisher, editor, or reporter.

b. Publishers, editors, or duly accredited reporters who are likewise personal information controllers or personal information processors within the meaning of the law are still bound to follow the Data Privacy Act and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.

Rule III. National Privacy Commission

Section 8. *Mandate*. The National Privacy Commission is an independent body mandated to administer and implement the Act, and to monitor and ensure compliance of the country with international standards set for personal data protection. Section 9. *Functions*. The National Privacy Commission shall have the following functions:

a. Rule Making. The Commission shall develop, promulgate, review or amend rules and regulations for the effective implementation of the Act. This includes:

1. Recommending organizational, physical and technical security measures for personal data protection, encryption, and access to sensitive personal information maintained by government agencies, considering the most appropriate standard recognized by the information and communications technology industry, as may be necessary;

2. Specifying electronic format and technical standards, modalities and procedures for data portability, as may be necessary;

3. Issuing guidelines for organizational, physical, and technical security measures for personal data protection, taking into account the nature of the personal data to be protected, the risks presented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, cost of security implementation, and the most appropriate standard recognized by the information and communications technology industry, as may be necessary;

4. Consulting with relevant regulatory agencies in the formulation, review, amendment, and administration of privacy codes, applying the standards set out in the Act, with respect to the persons, entities, business activities, and business sectors that said regulatory bodies are authorized to principally regulate pursuant to law;

5. Proposing legislation, amendments or modifications to Philippine laws on privacy or data protection, as may be necessary;

6. Ensuring proper and effective coordination with data privacy regulators in other countries and private accountability agents;

7. Participating in international and regional initiatives for data privacy protection.

b. Advisory. The Commission shall be the advisory body on matters affecting protection of personal data. This includes:

1. Commenting on the implication on data privacy of proposed national or local statutes, regulations or procedures, issuing advisory opinions, and interpreting the provisions of the Act and other data privacy laws;

2. Reviewing, approving, rejecting, or requiring modification of privacy codes voluntarily adhered to by personal information controllers, which may include private dispute resolution mechanisms for complaints against any participating personal information controller, and which adhere to the underlying data privacy principles embodied in the Act and these Rules;

3. Providing assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person, including the enforcement of rights of data subjects;

4. Assisting Philippine companies doing business abroad to respond to data protection laws and regulations.

c. Public Education. The Commission shall undertake necessary or appropriate efforts to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities. This includes:

1. Publishing, on a regular basis, a guide to all laws relating to data protection;

2. Publishing a compilation of agency system of records and notices, including index and other finding aids;

3. Coordinating with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal data in the country;

d. Compliance and Monitoring. The Commission shall perform compliance and monitoring functions to ensure effective implementation of the Act, these Rules, and other issuances. This includes:

1. Ensuring compliance by personal information controllers with the provisions of the Act;

2. Monitoring the compliance of all government agencies or instrumentalities as regards their security and technical measures, and recommending the necessary action in order to meet minimum standards for protection of personal data pursuant to the Act;

3. Negotiating and contracting with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

4. Generally performing such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;

5. Managing the registration of personal data processing systems in the country, including the personal data processing system of contractors and their employees entering into contracts with government agencies that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals.

e. Complaints and Investigations. The Commission shall adjudicate on complaints and investigations on matters affecting personal data: Provided, that In resolving any complaint or investigation, except where amicable settlement is reached by the parties, the Commission shall act as a collegial body. This includes:

1. Receiving complaints and instituting investigations regarding violations of the Act, these Rules, and other issuances of the Commission, including violations of the rights of data subjects and other matters affecting personal data;

2. Summoning witnesses, and requiring the production of evidence by a subpoena duces tecum for the purpose of collecting the information necessary to perform its functions under the Act: Provided, that the Commission may be given access to personal data that is subject of any complaint;

3. Facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, and adjudicating on matters affecting any personal data;

4. Preparing reports on the disposition of complaints and the resolution of any investigation it initiates, and, in cases it deems appropriate, publicizing such reports;

f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:

1. Issuing compliance or enforcement orders;

2. Awarding indemnity on matters affecting any personal data, or rights of data subjects;

3. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;

4. Recommending to the Department of Justice (DOJ) the prosecution of crimes and imposition of penalties specified in the Act;

5. Compelling or petitioning any entity, government agency, or instrumentality, to abide by its orders or take action on a matter affecting data privacy;

6. Imposing administrative fines for violations of the Act, these Rules, and other issuances of the Commission.

g. Other functions. The Commission shall exercise such other functions as may be necessary to fulfill its mandate under the Act.

Section 10. *Administrative Issuances*. The Commission shall publish or issue official directives and administrative issuances, orders, and circulars, which include:

a. Rules of procedure in the exercise of its quasi-judicial functions, subject to the suppletory application of the Rules of Court;

b. Schedule of administrative fines and penalties for violations of the Act, these Rules, and issuances or Orders of the Commission, including the applicable fees for its administrative services and filing fees;

c. Procedure for registration of data processing systems, and notification;

d. Other administrative issuances consistent with its mandate and other functions.

Section 11. *Reports and Information.* The Commission shall report annually to the President and Congress regarding its activities in carrying out the provisions of the Act, these Rules, and its other issuances. It shall undertake all efforts it deems necessary or appropriate to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities. Section 12. *Confidentiality of Personal Data*. Members, employees, and consultants of the Commission shall ensure at all times the confidentiality of any personal data that come to their knowledge and possession: Provided, that such duty of confidentiality shall remain even after their term, employment, or contract has ended. Section 13. *Organizational Structure.* The Commission is attached to the Department of Information and Communications Technology for policy and program coordination in accordance with Section 38(3) of Executive Order No. 292, series of 1987, also known as the Administrative Code of 1987. The Commission shall remain completely independent in the performance of its functions. The Commission shall be headed by a Privacy Commissioner, who shall act as Chairman of the Commission. The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Secretary. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners. One shall be responsible for Data Processing Systems, while the other shall be responsible for Policies and Planning. The Deputy Privacy Commissioners must be recognized

experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Undersecretary. Section 14. *Secretariat*. The Commission is authorized to establish a Secretariat, which shall assist in the performance of its functions. The Secretariat shall be headed by an Executive Director and shall be organized according to the following offices:

a. Data Security and Compliance Office;

b. Legal and Enforcement Office;

c. Finance and Administrative Office;

d. Privacy Policy Office;

e. Public Information and Assistance Office.

Majority of the members of the Secretariat, in so far as practicable, must have served for at least five (5) years in any agency of the government that is involved in the processing of personal data including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost). The organizational structure shall be subject to review and modification by the Commission, including the creation of new divisions and units it may deem necessary, and shall appoint officers and employees of the Commission in accordance with civil service law, rules, and regulations. Section 15. *Effect of Lawful Performance of Duty.* The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties: Provided, that they shall be liable for willful or negligent acts, which are contrary to law, morals, public policy, and good customs, even if they acted under orders or instructions of superiors: Provided further, that in case a lawsuit is filed against them in relation to the performance of their duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation. Section 16. *Magna Carta for Science and Technology Personnel*. Qualified employees of the Commission shall be covered by Republic Act No. 8349, which provides a magna carta for scientists, engineers, researchers, and other science and technology personnel in the government.

Rule IV. Data Privacy Principles

Section 17. *General Data Privacy Principles*. The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality. Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality*.

The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Section 19. *General principles in collection, processing and retention.* The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

a. Collection must be for a declared, specified, and legitimate purpose.

1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.

3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.

4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

b. Personal data shall be processed fairly and lawfully.

1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.

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

3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.

4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

c. Processing should ensure data quality.

1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.

2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

d. Personal Data shall not be retained longer than necessary.

1. Retention of personal data shall only for as long as necessary:

(a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;

(b) for the establishment, exercise or defense of legal claims; or

(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

2. Retention of personal data shall be allowed in cases provided by law.

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

e. Any authorized further processing shall have adequate safeguards.

1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.

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

3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Section 20. *General Principles for Data Sharing.* Further Processing of Personal Data collected from a party other than the Data Subject shall be allowed under any of the following conditions:

a. Data sharing shall be allowed when it is expressly authorized by law: *Provided*, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.

b. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:

1. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;

2. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.

(a) The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.

(b) The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject;

3. The data subject shall be provided with the following information prior to collection or before data is shared:

(a) Identity of the personal information controllers or personal information processors that will be given access to the personal data;

(b) Purpose of data sharing;

(c) Categories of personal data concerned;

(d) Intended recipients or categories of recipients of the personal data;

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

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

4. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.

c. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: Provided, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.

d. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement.

1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.

2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

Rule V. Lawful Processing of Personal Data

Section 21. *Criteria for Lawful Processing of Personal Information.* Processing of personal information is allowed, unless prohibited by law. For processing to be lawful, any of the following conditions must be complied with:

a. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;

b. The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;

c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

d. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;

e. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;

f. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or

g. The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

Section 22. *Sensitive Personal Information and Privileged Information*. The processing of sensitive personal and privileged information is prohibited, except in any of the following cases:

a. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;

b. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;

c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:

1. Processing is confined and related to the bona fide members of these organizations or their associations;

2. The sensitive personal information are not transferred to third parties; and

3. Consent of the data subject was obtained prior to processing;

e. The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or

f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

Section 23. *Extension of Privileged Communication*. Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered from privileged information is inadmissible. When the Commission inquires upon communication claimed to be privileged, the personal information controller concerned shall prove the nature of the communication in an executive session. Should the communication be determined as privileged, it shall be excluded from evidence, and the contents thereof shall not form part of the records of the case: *Provided*, that where the privileged communication itself is the subject of a breach, or a privacy concern or investigation, it may be disclosed to the Commission but only to the extent necessary for the purpose of investigation, without including the contents thereof in the records.
Section 24. *Surveillance of Suspects and Interception of Recording of Communications*. Section 7

of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended to include the condition that the processing of personal data for the purpose of surveillance, interception, or recording of communications shall comply with the Data Privacy Act, including adherence to the principles of transparency, proportionality, and legitimate purpose.

Rule VI. Security Measures for the Protection of Personal Data

Section 25. *Data Privacyand Security.* Personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data. The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law. The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

Section 26. *Organizational Security Measures.* Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security:

a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.

2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.

3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.

c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:

1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;

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

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

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

5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies.

e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:

1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable;

2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose;

3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems;

4. Policies and procedures for data subjects to exercise their rights under the Act;

5. Data retention schedule, including timeline or conditions for erasure or disposal of records.

f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject.

Section 27. *Physical Security Measures.* Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security:

a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

c. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;

d. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data;

e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Section 28. *Guidelines for Technical Security Measures.* Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:

a. A security policy with respect to the processing of personal data;

b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;

e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;

g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

Section 29. *Appropriate Level of Security.* The Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures, with the guidelines provided in these Rules and subsequent issuances of the Commission. In determining the level of security appropriate for a particular personal information controller or personal information processor, the Commission shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and may be updated as necessary by the Commission in separate issuances, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices.

Rule VII. Security of Sensitive Personal Information in Government

Section 30. *Responsibility of Heads of Agencies*. All sensitive personal information maintained by the government, its agencies, and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to these Rules and other issuances of the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein. The Commission shall monitor government agency compliance and may recommend the necessary action in order to satisfy the minimum standards. Section 31. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information*.

a. On-site and Online Access.

1. No employee of the government shall have access to sensitive personal information on government property or through online facilities unless he or she the employee has received a security clearance from the head of the source agency. The source agency is the government agency who originally collected the personal data.

2. A source agency shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access. An employee of the government shall

only be granted a security clearance when the performance of his or her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

3. Where allowed under the next preceding sections, online access to sensitive personal information shall be subject to the following conditions:

(a) An information technology governance framework has been designed and implemented;

(b) Sufficient organizational, physical and technical security measures have been established;

(c) The agency is capable of protecting sensitive personal information in accordance with data privacy practices and standards recognized by the information and communication technology industry;

(d) The employee of the government is only given online access to sensitive personal information necessary for the performance of official functions or the provision of a public service.

b. Off-site access.

1. Sensitive personal information maintained by an agency may not be transported or accessed from a location off or outside of government property, whether by its agent or employee, unless the head of agency has ensured the implementation of privacy policies and appropriate security measures. A request for such transportation or access shall be submitted to and approved by the head of agency. The request must include proper accountability mechanisms in the processing of data.

2. The head of agency shall approve requests for off-site access in accordance with the following guidelines:

(a) Deadline for Approval or Disapproval. The head of agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;

(b) Limitation to One thousand (1,000) Records. Where a request is approved, the head of agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the next succeeding paragraph.

(c) Encryption. Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

Section 32. *Implementation of Security Requirements.* Notwithstanding the effective date of these Rules, the requirements in the preceding sections shall be implemented before any off-site or online access request is approved. Any data sharing agreement between a source agency and another government agency shall be subject to review of the Commission on its own initiative or

upon complaint of data subject. Section 33. *Applicability to Government Contractors.* In entering into any contract with a private service provider that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, a government agency shall require such service provider and its employees to register their personal data processing system with the Commission in accordance with the Act and these Rules. The service provider, as personal information processor, shall comply with the other provisions of the Act and these Rules, particularly the immediately preceding sections, similar to a government agency and its employees.

Rule VIII. Rights of Data Subjects

Section 34. Rights of the Data Subject. The data subject is entitled to the following rights:

a. Right to be informed.

1. The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.

2. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:

(a) Description of the personal data to be entered into the system;

(b) Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;

(c) Basis of processing, when processing is not based on the consent of the data subject;

(d) Scope and method of the personal data processing;

(e) The recipients or classes of recipients to whom the personal data are or may be disclosed;

(f) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

(g) The identity and contact details of the personal data controller or its representative;

(h) The period for which the information will be stored; and

(i) The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

b. Right to object. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena;

2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or

3. The information is being collected and processed as a result of a legal obligation.

c. Right to Access. The data subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her personal data that were processed;

2. Sources from which personal data were obtained;

3. Names and addresses of recipients of the personal data;

4. Manner by which such data were processed;

5. Reasons for the disclosure of the personal data to recipients, if any;

6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;

7. Date when his or her personal data concerning the data subject were last accessed and modified; and

8. The designation, name or identity, and address of the personal information controller.

d. Right to rectification. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, That recipients or third parties who have previously

received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

e. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

1. This right may be exercised upon discovery and substantial proof of any of the following:

(a) The personal data is incomplete, outdated, false, or unlawfully obtained;

(b) The personal data is being used for purpose not authorized by the data subject;

(c) The personal data is no longer necessary for the purposes for which they were collected;

(d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;

(e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;

(f) The processing is unlawful;

(g) The personal information controller or personal information processor violated the rights of the data subject.

2. The personal information controller may notify third parties who have previously received such processed personal information.

f. Right to damages. The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

Section 35. *Transmissibility of Rights of the Data Subject*. The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section. Section 36. *Right to Data Portability*. Where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer. Section 37. *Limitation*

on Rights. The immediately preceding sections shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

Rule IX. Data Breach Notification.

Section 38. *Data Breach Notification.*

a. The Commission and affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that, a personal data breach requiring notification has occurred.

b. Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

c. Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

Section 39. *Contents of Notification*. The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects. Section 40. *Delay of Notification.* Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

a. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal data.

b. The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest, or in the interest of the affected data subjects.

c. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Section 41. *Breach Report.*

a. The personal information controller shall notify the Commission by submitting a report, whether written or electronic, containing the required contents of notification. The report shall also include the name of a designated representative of the personal information controller, and his or her contact details.

b. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually.

Section 42. *Procedure for Notification.* The Procedure for breach notification shall be in accordance with the Act, these Rules, and any other issuance of the Commission.

Rule X. Outsourcing and Subcontracting Agreements.

Section 43. *Subcontract of Personal Data*. A personal information controller may subcontract or outsource the processing of personal data: Provided, that the personal information controller shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission. Section 44. *Agreements for Outsourcing*. Processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.

a. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.

b. The contract or other legal act shall stipulate, in particular, that the personal information processor shall:

1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;

3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission;

4. Not engage another processor without prior instruction from the personal information controller: 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;

5. Assist the personal information controller, by appropriate 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;

6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;

7. At the choice of the personal information controller, delete or return all personal data to the personal information controller 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 Act or another law;

8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter;

9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

Section 45. *Duty of personal information processor.* The personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

Rule XI. Registration and Compliance Requirements

Section 46. *Enforcement of the Data Privacy Act.* Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the following:

a. Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals,

including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;

b. Notification of automated processing operations where the processing becomes the sole basis of making decisions that would significantly affect the data subject;

c. Annual report of the summary of documented security incidents and personal data breaches;

d. Compliance with other requirements that may be provided in other issuances of the Commission.

Section 47. *Registration of Personal Data Processing Systems.* The personal information controller or personal information processor that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

a. The contents of registration shall include:

1. The name and address of the personal information controller or personal information processor, and of its representative, if any, including their contact details;

2. The purpose or purposes of the processing, and whether processing is being done under an outsourcing or subcontracting agreement;

3. A description of the category or categories of data subjects, and of the data or categories of data relating to them;

4. The recipients or categories of recipients to whom the data might be disclosed;

5. Proposed transfers of personal data outside the Philippines;

6. A general description of privacy and security measures for data protection;

7. Brief description of the data processing system;

8. Copy of all policies relating to data governance, data privacy, and information security;

9. Attestation to all certifications attained that are related to information and communications processing; and

10. Name and contact details of the compliance or data protection officer, which shall immediately be updated in case of changes.

b. The procedure for registration shall be in accordance with these Rules and other issuances of the Commission.

Section 48. *Notification of Automated Processing Operations.* The personal information controller carrying out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes shall notify the Commission when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.

a. The notification shall include the following information:

1. Purpose of processing;

2. Categories of personal data to undergo processing;

3. Category or categories of data subject;

4. Consent forms or manner of obtaining consent;

5. The recipients or categories of recipients to whom the data are to be disclosed;

6. The length of time the data are to be stored;

7. Methods and logic utilized for automated processing;

8. Decisions relating to the data subject that would be made on the basis of processed data or that would significantly affect the rights and freedoms of data subject; and

9. Names and contact details of the compliance or data protection officer.

b. No decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of the data subject.

Section 49. *Review by the Commission.* The following are subject to the review of the Commission, upon its own initiative or upon the filing of a complaint by a data subject:

a. Compliance by a personal information controller or personal information processor with the Act, these Rules, and other issuances of the Commission;

b. Compliance by a personal information controller or personal information processor with the requirement of establishing adequate safeguards for data privacy and security;

c. Any data sharing agreement, outsourcing contract, and similar contracts involving the processing of personal data, and its implementation;

d. Any off-site or online access to sensitive personal data in government allowed by a head of agency;

e. Processing of personal data for research purposes, public functions, or commercial activities;

f. Any reported violation of the rights and freedoms of data subjects;

g. Other matters necessary to ensure the effective implementation and administration of the Act, these Rules, and other issuances of the Commission.

Rule XII. Rules on Accountability

Section 50. *Accountability for Transfer of Personal Data*. A personal information controller shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

a. A personal information controller shall be accountable for complying with the requirements of the Act, these Rules, and other issuances of the Commission. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a personal information processor or third party.

b. A personal information controller shall designate an individual or individuals who are accountable for its compliance with the Act. The identity of the individual or individuals so designated shall be made known to a data subject upon request.

Section 51. Accountability for Violation of the Act, these Rules and Other Issuances of the Commission.

a. Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the Act, these Rules, and other issuances of the Commission, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable.

b. In cases where a data subject files a complaint for violation of his or her rights as data subject, and for any injury suffered as a result of the processing of his or her personal data, the Commission may award indemnity on the basis of the applicable provisions of the New Civil Code.

c. In case of criminal acts and their corresponding personal penalties, the person who committed the unlawful act or omission shall be recommended for prosecution by the Commission based on substantial evidence. If the offender is a corporation, partnership, or any juridical person, the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime, shall be recommended for prosecution by the Commission based on substantial evidence.

Rule XIII. Penalties

Section 52. *Unauthorized Processing of Personal Information and Sensitive Personal Information.*

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

Section 53. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.*

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the Act or any existing law.

b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to sensitive personal information without being authorized under the Act or any existing law.

Section 54. *Improper Disposal of Personal Information and Sensitive Personal Information.*

a. A penalty of imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard, or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

b. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection.

Section 55. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.*

a. A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

b. A penalty of imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

Section 56. *Unauthorized Access or Intentional Breach.* A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored. Section 57. *Concealment of Security Breaches Involving Sensitive Personal Information.* A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Act, intentionally or by omission conceals the fact of such security breach. Section 58. *Malicious Disclosure.* Any personal information controller or personal information processor, or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00). Section 59. *Unauthorized Disclosure.*

a. Any personal information controller or personal information processor, or any of its officials, employees, or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

b. Any personal information controller or personal information processor, or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

Section 60. *Combination or Series of Acts*. Any combination or series of acts as defined in Sections 52 to 59 shall make the person subject to imprisonment ranging from three (3) years to six (6)

years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00). Section 61. *Extent of Liability*. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. Where applicable, the court may also suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 54 and 55 of these Rules, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be. Section 62. *Large-Scale.* The maximum penalty in the corresponding scale of penalties provided for the preceding offenses shall be imposed when the personal data of at least one hundred (100) persons are harmed, affected, or involved, as the result of any of the above-mentioned offenses. Section 63. *Offense Committed by Public Officer.* When the offender or the person responsible for the offense is a public officer, as defined in the Administrative Code of 1987, in the exercise of his or her duties, he or she shall likewise suffer an accessory penalty consisting of disqualification to occupy public office for a term double the term of the criminal penalty imposed. Section 64. *Restitution.* Pursuant to the exercise of its quasi-judicial functions, the Commission shall award indemnity to an aggrieved party on the basis of the provisions of the New Civil Code. Any complaint filed by a data subject shall be subject to the payment of filing fees, unless the data subject is an indigent. Section 65. *Fines and Penalties.* Violations of the Act, these Rules, other issuances and orders of the Commission, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with a schedule to be published by the Commission.

Rule XIV. Miscellaneous Provisions

Section 66. *Appeal.* Appeal from final decisions of the Commission shall be made to the proper courts in accordance with the Rules of Court, or as may be prescribed by law. Section 67. *Period for Compliance.* Any natural or juridical person or other body involved in the processing of personal data shall comply with the personal data processing principles and standards of personal data privacy and security already laid out in the Act. Personal information controllers and Personal Information processors shall register with the Commission their data processing systems or automated processing operations, subject to notification, within one (1) year after the effectivity of these Rules. Any subsequent issuance of the Commission, including those that implement specific standards for data portability, encryption, or other security measures shall provide the period for its compliance. For a period of one (1) year from the effectivity of these Rules, a personal information controller or personal information processor may apply for an extension of theperiod within which to comply with the issuances of the Commission. The Commission may grant such request for good cause shown. Section 68. *Appropriations Clause*. The Commission shall be provided with appropriations for the performance of its functions which shall be included in the General Appropriations Act. Section 69. *Interpretation.* Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner that would uphold the rights and

interests of the individual about whom personal data is processed. Section 70. *Separability Clause*. If any provision or part hereof is held invalid or unconstitutional, the remainder of these Rules or the provision not otherwise affected shall remain valid and subsisting. Section 71. *Repealing Clause.* Except as otherwise expressly provided in the Act or these Rules, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly. Section 72. *Effectivity Clause.* These Rules shall take effect fifteen (15) days after its publication in the Official Gazette.

Approved:

(Sgd.) RAYMUND E. LIBORO

Privacy Commissioner

(Sgd.) IVY D. PATDU

Deputy Privacy Commissioner

(Sgd.) DAMIAN DOMINGO O. MAPA

Deputy Privacy Commissioner

Promulgated: August 24, 2016