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 La Consolacion College Manila (LCCM) 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 College to protect data privacy rights, and shall serve as a guide in the exercise of rights under the DPA.

II. GENERAL PRIVACY POLICY STATEMENTS

1. La Consolacion College Manila 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 information is 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 The data subjects shall have the right to correct the information especially in cases of erroneous or outdated data, and to object to collection of personal information within the bounds allowed by privacy and education laws.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. LCCM 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. LCCM shall ensure that personal information is collected and processed only by authorized personnel for legitimate purposes of the College.
8. Any information that is declared obsolete based on the internal privacy and retention procedures of the College shall be disposed of in a secure and legal manner.
9. Any suspected or actual breach of the LCCM Data privacy policy must be reported to any member of the Data Privacy Response Team.

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 LCCM, including the data privacy and security policies implemented to ensure the protection of their personal data.

III. SCOPE AND LIMITATIONS

This Manual applies to all areas and departments of the College, 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 College. The data covered by this Manual is limited to **personal data**.

IV. PROCESSING OF PERSONAL DATA

1. Privacy Principles

1.1. 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. The collection of information is done with the consent of data subject (student and his/her guardian) which consent is included in the forms filled-out during application for admission, enrollment or availing of student services such as scholarships, on the job training).

1.2. FOR LEGITIMATE PURPOSE. In collecting personal information, the College shall use the information only for legitimate purposes. Only authorized personnel is allowed to access and process the personal information collected from the student, the parent or guardian in accordance with Data Privacy policies of the College and the Manual of Regulations for Private Higher Education which requires that student records as well as the information contained therein are to be kept confidential.

1.3. PROPORTIONALITY. Personal Information collected must be reasonably necessary or directly related to the College's functions. In the application for admission as a college student in LCCM, only information such as name, address, contact numbers, previous schools, parent's or guardian's name, which is necessary for the evaluation for eligibility for admission to the College is collected.

2. Provisions per Specific Office/Department/Unit

2.1. Office of Admission and Registrar's Office

The Office of Admissions and the Registrar's Office collects personal information for the purpose of evaluating the eligibility of the applicant for admission and/or enrollment in the college.

In the course of the collection of information, the authorized personnel from these offices ask the data subject (student and his/her parent or guardian to fill out forms with the corresponding privacy statement to signify consent and to inform him/her of the purpose of collecting such information during the admission and/ or enrollment processes). These offices collect, process the information and encode the same in the Student (profile) Data base. Only authorized personnel is allowed to encode and access student data.

2.2. Human Resource 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 (such as the retirement, study and medical benefits) and collates the information in the individual 201 files of the employees which is required under the provisions the Labor Code. Here, the individual employee 201 file is restricted only to authorized personnel in the Human Resource Department.

2.3. Health Services Unit

The Health Services Unit collects sensitive information relating to the medical and dental health of students and employees for monitoring pursuant to the provisions of the Manual of Regulations for Private Higher Education. And access to the data collected is restricted and limited only to authorized personnel in the unit.

2.4. Office of the Information Technology

The Office of the Information Technology processes and stores the data base system in the college. The data of student and employee given by the office/department is stored the records management system. Access to this data is also restricted and predetermined only by authorized personnel.

2.5. Other Offices/Departments/Units

The other offices/departments/units who will collect personal data from student or employee must always be subject to the policies provided in this manual.

3. Privacy Policies

To ensure the rights of the Data Subject to be protected:

3.1. The data subject is notified and his/her consent secured. Wherein, the collection of information is done with the consent of the data Subject (student and his/her guardian) 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 LCCM for legitimate purposes specifically for_____ and shall be processed by authorized personnel in accordance with the Data Privacy Policies of the College."*
>
> *"I hereby allow/authorize LCCM to use, collect and process my personal data for legitimate purposes specifically for _____, and allow authorized personnel in LCCM to process my personal data."*

3.2. Only authorized personnel is allowed to access and process the personal information collected from the student, his/her parent or guardian in accordance with Data Privacy policies of the College and the Manual of Regulations for Private Higher Education which requires that student records as well as the information contained therein are to be kept confidential.

V. SECURITY MEASURES

The College 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 College 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 for access to restricted student or employee records contained in the College information systems. As a general rule only authorized personnel with the necessary approvals may request for access of the information systems of personal 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. Only authorized personnel can open. The storage unit is placed in areas that are not usually accessible to the public, safe from physical hazards such as rain, wind and dust, and located in areas manned by the authorized personnel.

Various security appliances and devices are employed to safeguard the college network and its systems. And 24-hour security is also provided by the College to secure the areas where the College data center is located.

VI. USE AND DISCLOSURE OF PERSONAL INFORMATION

The authorized personnel of the college is allowed to access, use and process the personal data for legitimate purposes of the college and/or that which is stated in the privacy statement contained in the forms or documents signed by the employee or student.

The personal information is collected primarily for employment and educational purposes. Its use and disclosure for secondary purposes, such as his/her current health/psychological wellness, administrative or disciplinary standing, could be used as long as there is proper consent from the subject.

VII. RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

In accordance with the guidelines of the Manual of Regulations for Private and Higher Education, the college is required to indelibly take hold the employee and student records including the information contained therein. Hence, no personal information on this matter may be destroyed unless authorized and allowed by the college administration - with legal consent - and it must be documented in writing by the college.

In this regard, any unauthorized destruction should be reported to the Data Protection Officer and/or to any member of LCCM Data Privacy Response Team.

The manner of destruction will be done thru shredding of document records in order to avoid any reconstruction of the data.

VIII. INQUIRIES AND COMPLAINTS

The data subject may inquire or request for information regarding any matter in relation to his/her personal data to be processed. He/she may write the Data Protection Officer or any of the Personal Information Controllers regarding this inquiry or request.

The other rights of the data subject, as stated in the NPC Privacy Toolkit (May 2018 edition, page 89), are the following:

1. Right to dispute the inaccuracy or error in the personal data;
2. Right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and
3. Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

In case of a complaint for the violation of the Data Privacy Policy, the Data Protection Officer together with the Data Privacy Response Team, will conduct an investigation and verification of the violation/s of policies or data breach. The recommendation/decision shall be provided to the affected party and college President.

LCCM Data Privacy Response Team

Mr. Albert D. Manalili
Data Protection Officer
Tel. No. 8736-02-35 loc. 116
Email Address: albertmanalili@yahoo.com

Mr. Christopher A. de Luna
Personal Information Controller
Tel. No. 8736-02-35 loc. 134
Email Address: cadeluna@lccm.edu.com

Ms. Michelle E. Cortez
Personal Information Controller
Tel. No. 8736-02-35 loc. 104 / 87346487
Email Address: mick.cortez@gmail.com

Mr. Venancio N. Santos, Jr.
Personal Information Controller
Tel. No. 8736-02-35 loc. 107 / 53100564
Email Address: registrar@lccm.edu.ph

Mr. Richard L. Oliva
Personal Information Controller
Tel. No. 0945 3895203
Email Address: richard_r2j_oliva@lccm.edu.ph

Ms. Tonie Murielle A. Vidal
Personal Information Controller
Tel. No. 8736-02-35 loc. 115 / 53100513 to 14
Email Address: +vidal@lccm.edu.ph

Ms. Maria Liza V. Catan
Personal Information Controller
Tel. No. 8736-02-35 loc. 116
Email Address: hrd@lccm.edu.ph

IX. ANNEXES / APPENDICES

1. Privacy Notice

The La Consolacion College Manila is committed to protecting your privacy. This Privacy Notice explains how your personal information is collected, used, and disclosed by our institution.

We collect your information for employment (staffing, performance management, training, advancement plan) and enrollment (determining eligibility, contacting you about our academic programs/events, teaching, learning, processing necessary requirements to DepEd/CHED, maintain our alumni records).

By employment or enrolling in our institution, you signify that you have read, understood and agree to our collection, storage, use, and disclosure of your personal information as described in this Privacy Notice and our Terms of Service.

2. CCTV (Closed Circuit Television) Policy

Surveillance CCTV in school can play its part in meeting the reasonable expectations for all teachers, employees and students. Equally, regard must be paid to the rights of the individual for reasonable privacy and the avoidance of unacceptable, intrusive monitoring for whatever reason.

Location of CCTVs

CCTVs are sited so that they only capture images relevant to the purposes for which they have been installed (building premises and its associated equipments), and care will be taken to ensure that reasonable privacy expectations are not violated. The

school will make every effort to position the cameras so that their coverage is restricted to school premises, which include both indoor and outdoor areas.

Access to CCTV Images

The access to recorded images are restricted only to authorized personnel of LCCM to view them and will not be made widely available. And when CCTV recordings are being viewed, access will be limited to authorized personnel with authorization of Data Protection Officer on a need-to-know basis.

Subject Access Request

The data subject has the right to request CCTV footage relating to himself/herself under the Data Protection Act. He/she should put into writing the sufficient reason for this request to the Data Protection Officer (DPO). And the DPO will respond to this request within three (3) days of receiving the request.

Nevertheless, LCCM Administration reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of another individual or jeopardize an on-going investigation.

Procedures

The authorized personnel of LCCM for CCTV will:

a. Oversees and coordinate the use of CCTV monitoring for safety and security purposes;
b. Ensures that the CCTV monitoring is consistent with the highest standards and protections;
c. Reviews camera locations and be responsible for the release of any information stored in compliance with this policy and with due notice provided to the DPO;
d. Maintains a record of an access log;
e. Gives consideration to teachers, employees and students feedbacks/complaints regarding the operation/function of CCTV; and
f. Ensures that all areas being monitored by CCTV are not in breach of an enhanced expectation of the privacy of individuals within the school.

3. DISCLAIMER AND CONFIDENTIALITY NOTICE (Attached in LCCM e-mail)

The information contained in this email, including those in its attachments is confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the sender immediately and delete this email from your computer or system. If you are not the named recipient, you should not read, copy, store or distribute a copy of this email. Any views expressed in this email are those of the individual sender and may not necessarily reflect the views of La Consolacion College Manila.

4. Republic Act 10173 – Data Privacy Act of 2012

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:

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:

(1) 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 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.

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, in its 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 property or 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 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.

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) shall be 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 and subsisting.

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.