

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

15th Congress
First Regular Session

House Bill No. 1554

Introduced by Representative Roman T. Romulo
Lone District of Pasig City

EXPLANATORY NOTE

The Philippines does not have a unified and special law relating to the protection of the right of citizens to exercise choice to privacy and confidentiality of, and content control over, their personal information in both private and government information and communications systems.

This bill seeks: (1) to establish fair practices and regulation relating to the collection, use and protection of an individual's private information in both private and government information and communications systems, (2) to contribute to the promotion and development of electronic commerce in the Philippines, and to enhance the competitiveness of the Philippines in the international economy as a hub for business process outsourcing, and (3) to protect the consumers and promote consumer trust and user confidence in electronic commerce through the issuance of clear, transparent, predictable and enforceable rules to clarify and ensure the protection of personal data in information and communications systems in both the private sector and the government sector.

The undersigned believes that the passage of this bill will enhance the competitiveness of the Philippines in the international economy as a hub for business process outsourcing, and promote consumer trust and user confidence in electronic commerce.

For these reasons, the passage of this bill is earnestly sought.


ROMAN T. ROMULO

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

15th Congress

House Bill No. 1554

Introduced by Representative Roman T. Romulo
Lone District of Pasig City

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

Be it enacted by the Senate and the 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".

Section 2. Declaration of Policy. - It is the policy of the State to protect the fundamental human right of privacy of communication. The State likewise recognizes the vital role of information and communications technology in nation building but with its inherent obligation to ensure that personal information in information and communications systems in the government and the private sector are secure and protected.

Section 3. Interpretation. - Any doubt in the interpretation of any provision of this Act shall be interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

Section 4. Definition of Terms. -Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

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

"Personal information controller" means 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:

- a) a person or organization who performs such functions as instructed by another person or organization; and
- b) an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

"Processing" shall mean 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.

"Filing system" means any set of information relating to natural or juridical persons to the extent that, although the information is not processed by means of 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.

"Sensitive personal information" means personal information --

- a) about an individual's race, ethnic origin, marital status, age, color, religious, philosophical or political affiliations;
- b) which provide information as to the 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;
- c) which are 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;
- d) which have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"Privileged information" means any and all forms of data which under Section 24, Rule 130 of the Rules of Court and other pertinent laws, constitute privileged communication, specifically but not limited to those pertaining to communication exchanged in confidence between --

- a) Husband and wife;
- b) Lawyer and Client;
- c) Physician and Patient;
- d) Publisher, Editor or Reporter and their Informant;
- e) Parents and their Children.

"Data Subject" means an individual whose personal information is processed.

"Consent of the data subject" means any freely given, specific and informed expression of will, either in written or electronic form executed personally and voluntarily by the data subject, whereby the data subject agrees to the processing of personal information about and/or relating to him or her.

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

"Information and Communications System" means 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 in which data is recorded, transmitted or stored and any procedures related to the recording, transmission or storage of electronic data message or electronic document.

"Commission" shall refer to the National Privacy Commission created by virtue of this Act.

Sec. 5. 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 who, although not found or established in the Philippines, uses 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 further that the requirements of Section 6 is complied with.

This Act does not apply to the following:

- a) information about an 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 telephone number of the individual,
 - 3) the classification, salary range and responsibilities of the position held by the individual,
 - 4) the name of the individual on a document prepared by the individual in the course of employment, and
 - 5) the personal opinions or views of the individual given in the course of employment,
- b) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,
- c) information relating to any discretionary benefit of a financial nature given by the government, including the granting of a license or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit,
- d) personal information processed for personal or household and family purposes and where the personal information collected are not disclosed to other persons,
- e) personal information processed for journalistic, artistic or literary purposes.

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 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.
- 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

Section 7. Creation and Functions of the National Privacy Commission – A National Privacy Commission is hereby created 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, which 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 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 the prosecution and imposition of penalties of criminal offenses specified in this Act;
- j) review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers as well as other private sector self-regulatory initiatives, provided that the privacy codes or self-regulatory initiatives shall adhere to, and provide effective means of enforcing, the underlying data privacy principles embodied in this Act, and provided further that such privacy codes or self-regulatory initiatives may include private dispute resolution mechanisms for complaints against any participating personal information controller;
- 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, and, generally, perform such acts as may be necessary to facilitate cross-border enforcement of 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) report annually to the Congress and the President on the activities of the Commission in carrying out the provisions of this Act.

Section 8. Organizational Structure of the Commission - The Commission shall be attached to the Office of the President 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 six (6) years without reappointment. Of those first appointed, the Privacy Commissioner shall hold office for six (6) years, a Deputy Privacy Commissioner for three (3) years, and the last Deputy Privacy Commissioner for two (2) years, without reappointment.

The Privacy Commissioner must be a member of the Philippine Bar, at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, preferably with experience in Information Technology. 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 or data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

Section 9. Confidentiality – the Privacy Commissioner and the Deputy Privacy Commissioners shall ensure at all times the confidentiality of any personal information that comes to their knowledge and possession.

Section 10. Immunity. - Any violation of this Act shall subject them to criminal, civil and/or administrative sanction, provided however that no criminal or civil proceedings shall lie against the Privacy Commissioner, the Deputy Privacy Commissioners, or any person acting on their behalf or under their direction, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise of any duty or power under this Act.

SEC. 11. Vacancies - Vacancies in the membership of the Commission shall be filled in the same manner in which the original appointment was made. If there are at least two (2) members in office, vacancies in the membership of the Commission shall not impair the exercise of its powers and to execute its functions.

Sec. 12. Restriction on other employment – The members of the Commission may not engage in any other employment during their tenure as members of the Commission.

Sec. 13. Seal – The Commission shall have an official seal which shall be judicially noted.

Chapter III. PROCESSING OF PERSONAL INFORMATION

Sec. 14. 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, collecting personal information 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 the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing must be 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 as provided by law;
- 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 be 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.

Section 15. Criteria for Lawful Processing of Personal Information - The processing of personal information shall be permitted only if not otherwise prohibited by law, and at least one of the following conditions exist:

- a) the data subject has given his or her unambiguous consent which must be given in writing, or through any other similar means of express consent, according to the circumstances;
- 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; or
- e) the processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or when necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the personal information controller or in a third party to whom the data are disclosed.

Section 16. 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 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, and provided further, that the consent of the data subjects are not required by the law, or regulation permitting the processing of 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) processing is necessary to achieve the lawful, non-commercial objectives of public organizations and their associations, provided, 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, and provided finally, that consent of the data subject was obtained prior to processing;

- e) the processing is necessary for the 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.

Section 17. 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.

Section 18. Storage of Data - Personal information shall be stored and used only for as long as it is necessary to achieve the purpose for which it was processed, after which the personal information shall be deleted or blocked from a personal information base, unless otherwise provided by law.

Section 19. 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

Section 20. 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) before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity, be furnished the following:
 - i. description of the personal information to be entered into the system;
 - ii. purposes for which they are being or are to be processed;
 - iii. scope and method of the personal information processing;
 - iv. recipients or classes of recipients to whom they are or may be disclosed; and
 - v. methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized.

Any information supplied or declarations made to the data subject on these matters shall not be amended without prior notification of data subject; Provided further, the notification under letter (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes.

- c) be given reasonable access to, upon demand, the following:

- i. contents of his/her personal information that were processed;
 - ii. source from which personal information were obtained;
 - iii. names and addresses of recipients of the personal information;
 - iv. manner by which such data were processed;
 - v. reasons for the disclosure of the personal information to recipients;
 - vi. information on automated processes where the data will or is likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
 - vii. date when his or her personal information concerning the data subject were last accessed and modified;
 - viii. 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 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 recipients thereof provided further that third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject; or,
- 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, used for direct marketing purposes, unless expressly authorized, 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;
- f) be indemnified for any damages sustained by the latter due to such inaccurate, incomplete, outdated, false, unlawfully obtained, unauthorized use of personal information.

Sec. 21. Transmissibility of Rights of Data Subject – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for which s/he is an heir or assign 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. 22. 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 the same 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. 23. 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 –

- i. safeguards to protect its computer network against accidental, unlawful, or unauthorized usage or interference with or hindering of their functioning or availability;
- ii. a security policy with respect to the processing of personal information;
- iii. a process for identifying and assessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action for such vulnerabilities; and,
- iv. 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 representative of personal information controller and their representatives who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if these 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 that 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, prevent further disclosures, or to restore reasonable integrity to the information and communications system.

- i. In evaluating if notification is warranted, the Commission may take into account compliance by the personal information controller with Section 23 of this Act and existence of good faith in the acquisition of personal information.
- ii. 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.
- iii. 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

Section 24. Principle of Accountability. Each personal information controller is responsible for personal information under its control or custody, including information that has 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 is 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. 25. 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 on Information & Communications Technology. 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.

Section 26. Requirements relating to access by agency personnel to sensitive personal information -

(a) On-Site and On-line Access – Except as may be allowed through guidelines to be issued by the National Privacy Commission, no employee of the government shall have access to sensitive personal information on Government property or through on-line facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-Site Access – Until otherwise provided in guidelines to be issued by the National Privacy 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 procedure:

- (i) **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.
- (ii) **Limitation to 1,000 records -** If a request is approved, the head of the agency shall limit the access to not more than 1,000 records at a time.
- (iii) **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 on Information and Communications Technology.
- (iv) **Implementation-** The requirements of this subsection shall be implemented not later than 6 months after the date of the enactment of this Act.

Section 27. 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 the contractor and employees of the contractor to register their personal information processing system to 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. PENALTY PROVISIONS

Section 28. Offenses involving personal information – The National Privacy Commission may impose a fine of not less than Two Hundred Thousand Pesos (Php200,00.00) but not more than Two Million Pesos (Php 2,000,000) for each violation of Section 14 and of Section 19 of this Act in respect of personal information.

Section 29. Offenses involving sensitive personal information. The National Privacy Commission may impose a fine of not less than Five Hundred Thousand Pesos (Php500,00.00) but not more than Four Million Pesos (Php 4,000,000) for each violation of Section 14 and of Section 19 of this Act in respect of sensitive personal information.

Section 30. Other offenses – The National Privacy Commission may impose a fine of Two Hundred Thousand Pesos (Php 200,000.00) to Five Million Pesos (Php 5,000,000.00) for the following offenses:

- a) failure to issue a breach notification when warranted under Section 23(f);
- b) failure to implement appropriate security measures under Section 23; and
- c) other violations of this Act

Section 31. Commensurate to harm – The fines to be issued by the National Privacy Commission under Sections 28, 29 and 30 shall be commensurate to the severity of the harm caused, or likely to be caused by the offense under the circumstances.

Section 32. Criminal Action – Offenses involving personal information and sensitive personal information under Sections 28 and 29, when determined by the Department of Justice to be intentional in its separate and independent investigation, shall further be punishable by imprisonment ranging from one year to three years.

Chapter IX. MISCELLANEOUS PROVISIONS

Section 33. Implementing Rules and Regulations - Within ninety (90) days from the appointment of the Privacy Commissioners of the Commission, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

Sec. 34. 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. 35. Appropriations Clause - The Commission shall be provided with an initial appropriation of Twenty-Five Million Philippine Pesos (Php25,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act.

Sec. 36. Separability Clause - If any part or provision of this Act shall be held unconstitutional or invalid, other provisions hereof that are not affected thereby shall continue to be in full force and effect.

Sec. 37. Repealing Clause – The provision of Section 7 of Republic Act No. 9372 is hereby amended. All other laws, decrees, executive orders, proclamations and administrative regulations, or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Sec. 38. Effectivity Clause - This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation,

Approved.