FIFTEENTH CONGRESS OF THE REPUBLIC
OF THE PHILIPPINES

Second Regular Session

SENATE

COMMITTEE REPORT NO. 56

Submitted jointly by the Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws; Civil Service and Government Reorganization and Finance on SEP 14 2011.

Re: Senate Bill No. 2965

Recommending its approval in substitution of Senate Bill Nos. 355, 1908 and 2236, taking into consideration House Bill No. 4115.

Sponsor: Senator Edgardo J. Angara

MR. PRESIDENT:

The Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws and Finance to which were referred Senate Bill No. 355, introduced by Senator Trillanes, entitled:

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

S. No. 1908, introduced by Senator Defensor Santiago, entitled:

"AN
ACT TO ESTABLISH A PRIVACY PROTECTION COMMISSION"

S. No. 2236, introduced by Senator Defensor Santiago, entitled:

"AN ACT
TO INCREASE THE SECURITY OF SENSITIVE DATA MAINTAINED BY THE GOVERNMENT" and
House Bill No. 4115, introduced by Reps. Romulo, Roman T., Yap, Susan, Jalosjos, Cesar G., Tinga, Sigfrido R. and Palmones, Angelo B., entitled:

"AN ACT
PROTECTING INDIVIDUAL PERSONAL DATA IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND IN THE PRIVATE SECTOR, PROVIDING PENALTIES IN VIOLATION THEREOF, AND FOR OTHER PURPOSES"

have considered the same and have the honor to report them back to the Senate with the recommendation that the attached Senate Bill No. 2965, prepared by the Committees entitled:

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

be approved in substitution of Senate Bill Nos. 355, 1908, 2966, taking into consideration House Bill No. 4115, with Senators Trillanes, Defensor Santiago and Angara as authors thereof.
Respectfully submitted by:

Chairpersons

SEN. MIRIAM DEFENSOR-SANTIAGO
Chair
Committee on Constitutional Amendments,
Revision of Codes and Laws
Member, Committee on Finance
Committee on Science & Technology

SEN. EDGARDO J. ANGARA
Chair
Committee on Science and Technology
Chair, Subcommittee B
Vice Chair
Committee on Constitutional Amendments, Revision of Codes & Laws

SEN. FRANKLIN M. DRILON
Chair
Subcommittee A
Committee on Finance
Member
Committee on Constitutional Amendments, Revision of Codes & Laws

SEN. RALPH CORRECTO
Chair
Subcommittee C
Committee on Finance

SEN. ANTONIO “Sonny” F. TRILLANES IV
Chair
Committee on Civil Service and Government Reorganization
Member, Committee on Constitutional Amendments, Revision of Codes and Laws
Members

SEN. LOREN B. LEGARDA
Member
Committee on Science & Technology
Committee on Finance

SEN. FERDINAND R. MARCOS, JR.
Member
Committee on Science & Technology
Committee on Constitutional Amendments,
Revision of Codes & Laws
Committee on Finance

SEN. FRANCIS N. PANGILINAN
Member
Committee on Science & Technology
Committee on Finance

SEN. MANNY VILLAR
Member
Committee on Science & Technology
Committee on Constitutional Amendments,
Revision of Codes & Laws
Committee on Finance

SEN. PANFILO M. LACSON
Member
Committee on Constitutional Amendments, Revision of Codes
Committee on Finance

SEN. MANUEL M. "Lito" LAPID
Member
Committee on Constitutional Amendments,
Revision of Codes & Laws
Committee on Finance

SEN. FRANCIS G. ESCUDERO
Member, Committee on Finance
SEN. TEOFISTO L. GUINGONA III
Member
Committee on Finance

SEN. SERGIO R. OSMEÑA III
Member
Committee on Finance

SEN. JOKER P. ARROYO
Member
Committee on Finance

SEN. GREGORIO B. HONASAN
Member
Committee on Finance

SEN. RAMON REVILLA, JR.
Member
Committee on Finance

SEN. PIA S. CAYETANO
Member
Committee on Finance

SEN. AQUILINO "KOKO" PIMENTEL III
Member
Committees on Science and Technology and Finance
Ex-Officio Members

SEN. JINGGOY EJERCITO ESTRADA
Senate President pro-Tempore

SEN. VICENTE C. SOTTO III
Senate Majority Floor Leader

SEN. ALAN PETER S. CAYETANO
Senate Minority Floor Leader

SEN. JUAN PONCE ENRILE
Senate President
Pasay City
AN ACT

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

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

Chapter 1. GENERAL PROVISIONS

SECTION 1. Short Title.-This Act shall be known as the "Data Privacy Act of 2011."

SEC. 2. Declaration of Policy.- It is the policy of the State to protect the fundamental human right of privacy of communication. 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 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.

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 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.

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 in which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data 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 ascertained by the entity holding the information, or when put together with other information would 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 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.

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, color and religious, philosophical or political affiliations;

   (2) About an individual's health, genetic or sexual life of a person, or to any judicial 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 Philippine 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, further,* That the requirements of Section 5 are complied with.
This Act does not apply to the following:

(a) Information about all 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 agencies of their constitutionally and statutorily mandated functions.
(f) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

SEC. 5. 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;
   (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. 6. 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, 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) 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;

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

(f) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sec. 22 to 26 of This Act;

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

(h) 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, and provided further that such privacy codes may include private dispute
resolution mechanisms for complaints against any participating personal information controller.

SEC. 7. 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 three (3) years, and may 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 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 ICT and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

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. 8. 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, 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),
Chapter III. PROCESSING OF PERSONAL INFORMATION

SEC. 9. 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, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed 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;

(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, 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. 9-A. Principle of Accountability. – Each personal information controller is responsible 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.

SEC. 10. 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 exist:
(a) The data subject has given his or her express or implied 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; or
(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.
(f) The processing is necessary for the purposes of the legitimate interests pursued
by the 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. 11. 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 express consent, specific to the purpose prior to the 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. 12. 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. 13. 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 and all...
related purposes, after which the personal information shall be deleted or blocked from a personal information base, unless otherwise provided by law.

SEC. 14. 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. 15. 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; and

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

SEC. 16. 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. 17. 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. 18. Security of Personnel 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 assessing 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.

(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 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, 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. SECURITY OF SENSITIVE PERSONAL INFORMATION IN
GOVERNMENT

SEC. 19. 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. 20. 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. 21. 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, any 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 VII. PENALTIES

Sec. 22. 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 (P500,000.00) but not more than Two Million Pesos (P2,000,000.00) 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 (P500,000.00) but not more than Four Million Pesos (P4,000,000.00) 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. 23. 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 (P500,000.00) but not less or more than Two Million Pesos (P2,000,000.00) 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 (P500,000.00) but not more than Four Million Pesos (P4,000,000.00) 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. 24. 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 not less than One Hundred Thousand Pesos (Php 100,000.00) but not more than Five Hundred Thousand Pesos (Php 500,000.00) 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 not less than One Thousand Pesos (Php 100,000.00) but not more than One Million Pesos (Php 1,000,000.00) 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. 25. Wrongful Processing of Personal Information and Sensitive Personal Information.

a) 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 (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) 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.

b) 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 not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00) 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.
SEC. 26. 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 (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) 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.

8a) 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 (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00) 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.

SEC. 27. Unauthorized Access or Intentional Breach. - The penalty of imprisonment ranging from one (1) year to three (3) years and a fine not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00) 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. 28. Concealment of Security Breaches Involving Sensitive Personally Identifiable 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 (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 18 (f), intentionally or by omission conceals the fact of such security breach.

SEC. 29. Malicious Disclosure. - Any person 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 from a data controller or unknowingly transferred to him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years imprisonment and a fine of not less than Five
Hundred Thousand Pesos (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00).

SEC. 30. Unauthorized Disclosure. -

a) Any person who discloses to a third party personal informal not covered by the immediately preceding section without the consent of the data subject obtained by him from a data controller or unknowingly transferred to him, shall be subject to imprisonment ranging from one (1) year to three (3) years imprisonment and a fine of not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than One Million Pesos (Php 1,000,000.00).

b) Any person who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject obtained by him from a data controller or unknowingly transferred to him, shall be subject to imprisonment ranging from three (3) years to five (5) years imprisonment and a fine of not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00).

SEC. 31. Breach of Confidentiality. - The penalty of imprisonment ranging from two (2) years and four (4) months to five (5) years and a fine not less than Five Hundred Thousand Pesos (Php 500,000.00) but not more than Two Million Pesos (Php 2,000,000.00) shall be imposed in case of a breach of confidentiality where such breach has resulted in the information being published or reported by media. In this case, the responsible reporter, writer, president, publisher, manager and editor-in-chief shall be liable under this Act.

SEC. 32. Combination of Series of Acts. - Any combination or series of acts as defined in Section 23 to 30 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 (Php 1,000,000.00) but not more than Five Million Pesos (Php 5,000,000.00).

SEC. 33. 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 shall, in addition to the penalties
herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and he is found guilty of acts penalized under Section 24 and 25 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. 34. 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. 35. 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 duties, an accessory penalty consisting in the disqualification to occupy public offices for a term double the term of criminal penalty imposed shall be applied.

SEC. 36. Restitution. – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

Chapter VIII. MISCELLANEOUS PROVISIONS

SEC. 37. Interpretation. - Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in favor of the rights and interests of the individual whose personal information are processed.

SEC. 38. Implementing Rules and Regulations. – Within ninety (90) days from effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 39. 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. 40. Appropriations Clause. – The Commission shall be provided with an initial appropriation of Twenty Million Pesos (Php 20,000,000.00) 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 (Php 10,000,000.00) per year for five years upon implementation of this Act drawn from the national government.

SEC. 41. Transitory Period. - 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 determined by the Commission, to comply with the requirements of this Act.

SEC. 42. 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. 43. Repealing Clause. – The provision of Section 7 of Republic Act No. 9372, otherwise known as the “Human Security Act of 2007”, 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. 44. Effectivity Clause. – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Approved,